Cisco Secure Email Threat Defense ユーザーガイド

目次

はじめに 7

要件 9

Secure Email Threat Defense の設定 11
- アカウントへのサインイン 11
- Cisco Secure Email Gateway（SEG）の有無を表示 11
- メッセージの送信元、可視性と修復モードの選択 11
- メッセージの送信元の設定 12
  - メッセージの送信元：Microsoft O365 13
  - メッセージの送信元：ゲートウェイ 14
- ポリシー設定の確認 14
- Microsoft の電子メールドメインのインポート 14
  - 手動インポート 15
  - 自動インポート 15

ポリシー設定 17
- ゲートウェイを使用している場合のポリシー設定 19
- メッセージの送信元の切り替え 20

メッセージ 21
- [メッセージ（Messages）] ページのアイコン 21
- 検索およびフィルタ 22
  - [フィルタ（Filter）] パネル 22
  - メッセージグラフとクイックフィルタ 23
- 判定 23
  - レトロスペクティブな判定 24
    - レトロスペクティブな判定の電子メール通知 24
- メッセージレポート 24
  - タイムライン 25
  - 判定と手法 26
  - 送信者情報 26
  - 送信者メッセージ 26
  - 受信者情報 27
  - メールボックスリスト 27
  - リンクと添付ファイル 27

電子メールのプレビュー . . . 28
カンバセーションビュー . . . 28
XDR ピボットメニュー . . . 29
メッセージの移動と再分類 . . . 29
ハイブリッド Exchange アカウントについて . . . 29
読み取り修復モード . . . 29
読み取り/書き込み修復モード . . . 30
メッセージを削除する . . . 31
メッセージの隔離 . . . 31
検索結果のダウンロード . . . 32
ダウンロード履歴 . . . 33

ダウンロード . . . 35
メッセージ . . . 35
EML ダウンロード . . . 36
修復エラーログ . . . 36

インサイト . . . 39
トレンド . . . 39
タイムゾーンについて . . . 39
宛先別メッセージ . . . 40
脅威 . . . 41
スパム . . . 41
グレイメール . . . 41
影響レポート . . . 41

影響力の高い人員リスト . . . 45
影響力の高い人員リストにユーザーを追加する . . . 45
影響力の高い人員リストのユーザー情報を更新する . . . 45
影響力の高い人員リストからユーザーを削除する . . . 45

ユーザーの管理 . . . 47
マルチアカウントアクセス . . . 47
ユーザーロール . . . 47
新規ユーザーの作成 . . . 50
ユーザの編集 . . . 50
ユーザの削除 . . . 51

ユーザー設定 . . . 53
詳細 . . . 53
初期設定 . . . 53
XDR リボン . . . 53
テーマ . . . 53

管理設定 . . . 55
アカウント . . . 55
ライセンス . . . 55
初期設定 . . . 55
通知メール . . . 55
監査ログ . . . 56
Google アナリティクス . . . 56
Cisco XDR . . . 56

メッセージルール . . . 57
許可リストルール . . . 57
判定のオーバーライドルール . . . 58
バイパス分析ルール . . . 58
バイパスルールの作成と使用に関するアドバイザリ . . . 58
メッセージルールの追加 . . . 59
新しい許可リストまたは判定のオーバーライドルールの追加 . . . 59
新しいバイパス分析ルールの追加 . . . 59
ルールの編集 . . . 60
ルールの有効化または無効化 . . . 60
ルールの削除 . . . 60
Microsoft 許可リストと安全な送信者 . . . 61

Cisco XDR . . . 63
XDR . . . 63
Secure Email Threat Defenseの Cisco XDR の承認 . . . 63
Secure Email Threat Defenseの XDR 承認の取り消し . . . 64
XDR リボン . . . 64
ピボットメニュー . . . 64
XDR リボンの承認 . . . 65
XDR リボンの承認の取り消し . . . 65

API . . . 67

Secure Email Threat Defense の無効化 . . . 69
メッセージの送信元：Microsoft 365 . . . 69
Cisco Secure Email Threat Defense ジャーナルルールの削除 . . . 69
Azure からの Cisco Secure Email Threat Defense アプリケーションの削除 . . . 69
メッセージの送信元：ゲートウェイ . . . 69
メッセージの送信を停止するようにゲートウェイを構成する . . . 70
Azure からの Cisco Secure Email Threat Defense アプリケーションの削除 . . . 70

よく寄せられる質問（FAQ） . . . 71

はじめに

Cisco Secure Email Threat Defense は、Microsoft 365 向けの統合型クラウドネイティブ セキュリティ ソリューションで、シンプルな導入、簡単な攻撃修復、優れた可視性に重点を置いています。

要件

Cisco Secure Email Threat Defense を正常に設定して使用するための要件は次のとおりです。

- Cisco Secure Email Threat Defense を購入し、ウェルカムメールを受信している。
- 次のいずれかのブラウザの最新バージョンを使用している。
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- メッセージの送信元が Microsoft 365 であるか、可視性と修復モードで Microsoft 365 認証を使用している場合:
  - グローバル管理者権限を持つ Microsoft 365 アカウントを所有している。
  - 配信不能なジャーナルレポートを受信できる Microsoft 365 環境の電子メールアドレスを所有している。使用される電子メールアドレスはジャーナリングされません。Cisco Secure Email Threat Defense の分析対象とするアドレスを使用しないでください。

Secure Email Threat Defense の設定

Cisco Secure Email Threat Defense の設定には、次の手順が含まれます。

1. アカウントへのサインイン（11 ページ）
2. Cisco Secure Email Gateway（SEG）の有無を表示（11 ページ）
3. メッセージの送信元、可視性と修復モードの選択（11 ページ）
4. メッセージの送信元の設定（12 ページ）
5. ポリシー設定の確認（14 ページ）
6. Microsoft の電子メールドメインのインポート（14 ページ）

次の手順は、**要件（9 ページ）**を満たしていることを前提としています。

アカウントへのサインイン

1. シスコからのウェルカムメールの指示に従って、ユーザーアカウントを設定します。

   Cisco Secure Email Threat Defense は、Cisco Security Cloud Sign On を使用してユーザー認証を管理します。Security Cloud Sign On サインオンの詳細については、https://cisco.com/go/securesignon を参照してください。既存の SecureX Threat Response、Cisco Secure Malware Analytics（旧 Threat Grid）、または Cisco Secure Endpoint（旧 AMP）のお客様は、既存のクレデンシャルでサインインしてください。既存のユーザーでない場合は、新しい Security Cloud Sign On アカウントを作成する必要があります。

2. サインインに成功したら、利用規約に同意します。
3. [ようこそ（Welcome to）] **Cisco Secure Email Threat Defense**ページにアクセスできるようになりました。次のセクションで説明されているように、セットアップウィザードに従います。

Cisco Secure Email Gateway（SEG）の有無を表示

（次のセクションで選ぶ）メッセージの送信元が何であれ、Cisco Secure Email Gateway（SEG）が存在することと、受信ジャーナルでの SEG の識別に使用できるヘッダーを示すことにより、Cisco Secure Email Threat Defense でメッセージの真の発信者を特定できるようにすることが重要です。この設定を行わないと、SEG から送信されたすべてのメッセージが表示され、誤検出が発生する可能性があります。

1. [はい（Yes）] または [いいえ（No）] を選択して Cisco Secure Email Gateway（SEG）が存在するかどうかを確認し、[次へ（Next）] をクリックします。
2. [はい（Yes）] と答えた場合は、SEG のタイプとヘッダーを入力します。[次へ（Next）] をクリックします。

メッセージの送信元、可視性と修復モードの選択

1. メッセージの送信元を、Microsoft O365 またはゲートウェイのいずれかから選択します。前の手順で [SEGはありません（No SEG）] を選択した場合、メッセージの送信元には Microsoft O365 が選択されていると想定されます。
2. 可視性と修復を選択します。

可視性と修復モードは、適用できる修復ポリシーのタイプを定義します。

Microsoft 365 認証

- **読み取り/書き込み（Read/Write）**：可視性、およびオンデマンドまたは自動の修復（疑わしいメッセージの移動または削除）が可能です。読み取り/書き込み権限が Microsoft 365 から要求されます。
- **読み取り（Read）**：可視性のみを許可し、修復は許可しません。読み取り専用権限が Microsoft 365 から要求されます。

  注：[読み取り/書き込み（Read/Write）] を選択した場合は、セットアップの完了後に **ポリシー設定（17 ページ）** で自動修復ポリシーをオンにする必要があります。すべての内部電子メールに自動修復を適用するには、[ポリシー（Policy）] ページの [ドメインリストにないドメインに自動修復を適用する（Apply auto-remediation to domain not in domain list）] ボックスがオンに設定されていることを確認します。

Microsoft 365 認証モードでは、Cisco Secure Email Threat Defense から Microsoft によるアクセス許可を要求します。これらの許可は、読み取り/書き込みモードと読み取りモードのどちらを選択したかによって異なります。アクセス許可の詳細については、リンクされている Microsoft のドキュメントを参照してください。

両方の Microsoft 認証モードからの要求：**Organization.Read.All** および **User.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#organizationreadall
- https://learn.microsoft.com/en-us/graph/permissions-reference#userread

読み取り/書き込みモードからの要求：**Mail.ReadWrite**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailreadwrite

読み取りモードからの要求：**Mail.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailread

認証なし（No Authentication）

このオプションは、メッセージの送信元として Cisco SEG を使用している場合に使用できます。可視性のみを提供します。メッセージを修復することはできません。

3. Microsoft 365 認証を選択した場合は、Microsoft 365 に接続します。
   a. [次へ（Next）] をクリックして Microsoft 365 に接続します。
   b. 指示に従って、Microsoft 365 アカウントにログインします。このアカウントにはグローバル管理者権限が必要です。Cisco Secure Email Threat Defense ではアカウントの保存または使用は実行されません。これらの権限が必要な理由については、Cisco Secure Email Threat Defense の FAQ「Why are Microsoft 365 Global Admin rights required to set up Secure Email Threat Defense?」を参照してください。
   c. [承認（Accept）] をクリックして、Cisco Secure Email Threat Defense アプリケーションの権限を承認します。Cisco Secure Email Threat Defense の設定ページにリダイレクトされます。
   d. [次へ（Next）] をクリックします。

メッセージの送信元の設定

選択したメッセージの送信元の手順を完了します。

メッセージの送信元：Microsoft O365

メッセージの送信元に Microsoft O365 を選択した場合は、ジャーナルを Cisco Secure Email Threat Defense へ送信するように Microsoft 365 を設定する必要があります。これを行うには、ジャーナルルールを追加します。ゲートウェイを配置している場合は、ジャーナルルールを追加する前に、Microsoft 365 にコネクタを追加します。

1. **Cisco Secure Email Gateway（SEG）を使用しているユーザーの場合**：Microsoft 365 にコネクタを追加します。

   ジャーナルが Cisco Secure Email Gateway を経由することなく、Microsoft 365 から Cisco Secure Email Threat Defense に直接送信されるようにするため、Microsoft 365 に送信コネクタを追加することを推奨します。コネクタはジャーナルを設定する前に追加する必要があります。

   Microsoft 365 Exchange 管理センターから、[コネクタの追加（Add a connctor）] ウィザードの次の設定を使用して新しいコネクタを作成します。

   - [接続元（Connection from）]：Office 365。
   - [接続先（Connection to）]：パートナー組織。
   - [コネクタ名（Connector name）]：Cisco Secure Email Threat Defense へのアウトバウンド（[オンにする（Turn it on）] チェックボックスを選択）。
   - [コネクタの使用（Use of connector）]：電子メールメッセージがこれらのドメインに送信される場合のみ（北米環境の場合は **mail.cmd.cisco.com**、ヨーロッパ環境の場合は **mail.eu.cmd.cisco.com**、オーストラリア環境の場合は **mail.au.etd.cisco.com**、インド環境の場合は **mail.in.etd.cisco.com** を追加）。
   - [ルーティング（Routing）]：パートナーのドメインに関連付けられた MX レコードを使用。
   - [セキュリティの制限（Security restrictions）]：接続を保護するために、信頼できる認証局（CA）によって発行されたトランスポート層セキュリティ（TLS）を常に使用（推奨）。
   - [検証用の電子メール（Validation email）]：Cisco Secure Email Threat Defense の設定ページのジャーナルアドレス。

     注：O365 テナントで、Exchangeトランスポートルールを使用して、送信メールを既存のコネクタにルーティングする条件付きメールルーティングがすでに設定されている場合、コネクタ検証に失敗することがあります。ジャーナルメッセージにはシステム特権があり、トランスポートルールの影響を受けませんが、コネクタ検証テストの電子メールには特権がなく、トランスポートルールの影響を受けます。

     この検証の問題を解決するには、既存のトランスポートルールを見つけて、Cisco Secure Email Threat Defense ジャーナルアドレスの例外を追加します。この変更が有効になるのを待ってから、新しいコネクタの検証を再テストしてください。

2. Cisco Secure Email Threat Defense にジャーナルを送信するように Microsoft 365 を設定します。これを行うには、ジャーナルルールを追加します。

   a. Cisco Secure Email Threat Defense の設定ページから、ジャーナルアドレスをコピーします。後でこのプロセスを繰り返す必要がある場合は、[管理（Administration）] ページでジャーナルアドレスを確認することもできます。

   b. Microsoft Purview コンプライアンスポータル（https://compliance.microsoft.com/homepage）に移動します。

   c. [ソリューション（Solutions）] > [データライフサイクル管理（Data lifecycle management）] > [Exchange（レガシー）（Exchange (legacy)）] > [ジャーナルルール（Journal rules）] の順に移動します。

   d. まだ実行していない場合は、[配信不能ジャーナルレポートの送信先（Send undeliverable journal reports to）] フィールドに Exchange の受信者を追加して、[保存（Save）] をクリックします。使用される電子メールアドレスはジャーナリングされません。Cisco Secure Email Threat Defense の分析対象とするアドレスを使用しないでください。この目的で使用する受信者がいない場合は、受信者を作成する必要があります。

   e. [ジャーナルルール（Journal rules）] ページに戻ります。[+] ボタンをクリックして、新しいジャーナルルールを作成します。

f. Cisco Secure Email Threat Defense の設定ページのジャーナルアドレスを [ジャーナルレポートの送信先(Send journal reports to)] フィールドに貼り付けます。

g. [ジャーナルルール名(Journal rule name)] フィールドに「**CiscoCisco Secure Email Threat Defense**」と入力します。

h. [ジャーナルメッセージの送受信元(Journal messages sent or received from)] で、[全員(Everyone)] を選択します。

i. [ジャーナルするメッセージのタイプ(Type of message to journal)] で、[すべてのメッセージ(All messages)] を選択します。

j. **[次へ(Next)]** をクリックします。

k. 選択内容を確認してから、[送信(Submit)] をクリックしてルールの作成を終了します。

3. Cisco Secure Email Threat Defense の設定ページに戻ります。[ポリシーの確認(Review policy)] をクリックします。

メッセージの送信元:ゲートウェイ

メッセージの送信元にゲートウェイを選択した場合は、Cisco Secure Email Cloud Gateway の Threat Defense コネクタを有効にし、メッセージを Secure Email Threat Defense に送信できるようにします。

1. Cisco Secure Email Threat Defense の設定ページから、メッセージ受信アドレスをコピーします。後でこのプロセスを繰り返す必要がある場合は、[管理(Administration)] ページでメッセージ受信アドレスを確認できます。
2. Cisco Secure Email Cloud Gateway UI から、[セキュリティサービス(Security Services)] > [Threat Defense Connector] の順に選択します。
3. [Threat Defense Connectorの有効化(Enable Threat Defense Connector)] チェックボックスをオンにします。
4. 手順 1 で Cisco Secure Email Threat Defense からコピーしたメッセージ受信アドレスを入力します。
5. [送信(Submit)] をクリックして変更を確定します。
6. Cisco Secure Email Threat Defense の設定ページに戻ります。[ポリシーの確認(Review policy)] をクリックします。

ポリシー設定の確認

ポリシー設定については、**ポリシー設定(17 ページ)**を参照してください。[Microsoft O365 認証:読み取り/書き込み(Microsoft O365 Authentication: Read/Write)] モードを選択した場合は、[自動修復(Automated Remediation Policy)] の設定も確認する必要があります。すべての内部電子メールに自動修復を適用するには、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domain not in domain list)] がオンに設定されていることを確認します。ドメインがインポートされたら、**自動修復ポリシー**の切り替えをオンにできます。

Microsoft の電子メールドメインのインポート

Cisco Secure Email Threat Defense は、Microsoft 365 テナントから電子メール機能を持つドメインをインポートします。ドメインをインポートして、特定のドメインに自動修復を適用できるようにします。Cisco Secure Email Threat Defense は、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] ボックスがオンかオフかによって、新しくインポートされたドメインを異なる方法で処理します。

- [ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] がオンになっている場合、インポートされるすべての新しいドメインに自動修復が適用されます。
- [ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] がオフになっている場合、インポートされる新しいドメインに自動修復は適用されません。

デフォルトでは、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] はオフになっています。

手動インポート

Microsoft 365 電子メールドメインを手動でインポートするには、次の手順を実行します（Cisco Secure Email Threat Defense の初回セットアップ時に推奨）。

1. **[ポリシー（Policy）]** ページに移動します。
2. [インンポートされたドメインの更新（Update Imported Domains）] ボタンをクリックし、ドメインを Cisco Secure Email Threat Defense にインポートします。
3. 各ドメインの横にあるチェックボックスを使用して、そのドメインの自動修復設定を調整します。
4. また、[ドメインリストにないドメインに自動修復を適用する（Apply auto-remediation to domains not in the domain list）] を選択して、自動修復がすべての内部メールと後で自動的にインポートされるドメインに適用されるようにすることもお勧めします。
5. [保存して適用（Save and Apply）] をクリックします。

自動インポート

リストを最新にするために、ドメインは 24 時間ごとに自動的にインポートされます。

ポリシー設定

[ポリシー(Policy)] ページの設定によって、Cisco Secure Email Cloud Mailbox でのメールの処理方法が決まります。**Secure Email Threat Defense の設定(11 ページ)** の手順では、デフォルト設定が適用されます。設定を変更するには、変更を行い、[保存して適用(Save and Apply)] ボタンをクリックします。

表 1　　ポリシー設定

設定	説明	オプション	デフォルト
メッセージの送信元(Message Source)	メッセージの送信元を定義します。	■ **Microsoft 365** ■ **Gateway(ゲートウェイ)**(着信メッセージのみ)	Cisco Secure Email Threat Defense を設定するときに手動で選択します。
可視性と修復(Visibility & Remediation)	適用できる修復ポリシーのタイプを定義します。	■ **Microsoft 365 認証(Microsoft 365 Authentication)** – 読み取り/書き込み(Read/Write):可視性、およびオンデマンドまたは自動の修復(疑わしいメッセージの移動または削除)が可能です。読み取り/書き込み権限が Microsoft 365 から要求されます。 – 読み取り(Read):可視性のみを許可し、修復は許可しません。読み取り専用権限が Microsoft 365 から要求されます。 [読み取り(Read)] を選択した場合は、[添付ファイルの分析(Attachment Analysis)] および [メッセージの分析(Message Analysis)] の方向のみ設定する必要があります。修復ポリシーは適用されません。 ■ **認証なし(No Authentication)** 可視性のみを許可します。	Cisco Secure Email Threat Defense を設定するときに手動で選択します。 [Microsoft 365 認証(Microsoft 365 Authentication)] 設定を変更すると、Microsoft 365 の権限をリセットするようにリダイレクトされます。 ジャーナリングを設定するように指示される場合もあります。すでにジャーナリングを設定している場合は、この手順を省略できます。 **注:** [Microsoft 365 認証:読み取り/書き込み(Microsoft 365 Authentication: Read/Write)] を選択した場合は、[自動修復ポリシー(Automated Remediation Policy)] の設定も確認する必要があります。
Cisco Secure Email Gateway(SEG)	Cisco Secure Email Gateway(SEG)の有無は、Secure Email Threat Defense が送信者 IP を識別する方法に影響します。	■ 何も選択されていません(SEGはありません)(Nothing selected (No SEG)) ■ **SEGがあります(SEG is present)** – Cisco SEGのデフォルトヘッダーを使用する(Use Cisco SEG default header)(X-IronPort-RemoteIP)。 – SEGのカスタムヘッダーを使用する(Use Custom SEG header)。使用するヘッダーを追加する必要があります。	Cisco Secure Email Threat Defense を設定するときに手動で選択します。 詳細については、ゲートウェイを使用している場合のポリシー設定(19 ページ)を参照してください。

表 1　　ポリシー設定

設定	説明	オプション	デフォルト
メッセージの分析（Message Analysis）	動的に分析されるメッセージ。次のものが含まれます。 ■ メッセージの方向（Direction of messages） ■ Cisco Secure Malware Analytics によって分析されるメールの添付ファイルの方向 ■ スパムとグレイメールの分析（Analysis of Spam and Graymail）	■ **メッセージの方向（Direction of Messages）** – **着信（Incoming）** – **発信（Outgoing）** – **内部（Internal）** ■ **添付ファイルの方向（Direction of Attachments）** – **着信（Incoming）** – **発信（Outgoing）** – **内部（Internal）** ■ **スパムおよびグレイメール（Spam and Graymail）** – [オン（On）] または [オフ（Off）]	■ **メッセージの方向（Direction of Messages）** – メッセージの送信元が Microsoft O365 の場合は [すべて（All）] – メッセージの送信元がゲートウェイの場合は [着信（Incoming）] ■ **添付ファイルの方向（Direction of Attachments）** – **着信（Incoming）** ■ **スパムおよびグレイメール（Spam and Graymail）** – 2023 年 5 月 9 日以降に作成されたすべてのアカウントで [オフ（Off）]
自動修復ポリシー（Automated Remediation Policy）	次であることが判明したメッセージの修復アクション： ■ **脅威**（BEC、詐欺、フィッシング、または悪意のある） ■ **Spam** ■ **グレイメール**	■ **アクションなし（No Action）** ■ **隔離に移動（Move to Quarantine）** ■ **ゴミ箱に移動（Move to Trash）** ■ **迷惑メールに移動（Move to Junk）** **注**：送信者アドレスが Exchange の送信者許可リストに属している場合、またはメッセージが Microsoft 365 によってすでに修復されている場合、修復アクションは適用されません。	■ [自動修復ポリシー（Automated Remediation Policy）] の切り替え：オフ ■ 脅威：[隔離に移動（Move to Quarantine）] ■ [スパム（Spam）] - [迷惑メールに移動（Move to Junk）] ■ [グレイメール（Graymail）] - [アクションなし（No Action）]
Safe Sender：Microsoft Safe Sender メッセージをスパムまたはグレイメールの判定で修復しないでください。	このボックスがオンになっている場合、ジャーナルヘッダーで Microsoft により Safe Sender としてタグ付けされたメッセージのうち、Secure Email Threat Defense によってスパムまたはグレイメールと判定されたものは修復されません。	[選択（Checked）] または [選択解除（Unchecked）]	**選択解除（Unchecked）**

表 1　　ポリシー設定

設定	説明	オプション	デフォルト
インポート済みのドメイン：メッセージの方向を決定するためにドメインがインポートされます。自動修復ポリシーからドメインを除外できます。			
自動修復の適用（Apply Auto-Remediation）	特定のドメインに自動修復を適用します。	[選択（Checked）] または [選択解除（Unchecked）]	選択解除（Unchecked）。[読み取り/書き込み（Read/Write）] 修復モードをオンにする場合は、これらのチェックボックスをオンにして特定のドメインに自動修復が適用されるようにします。
上のドメインリストにないドメインに自動修復を適用する（Apply auto-remediation to domains not in the domain list above）	ドメインが明示的にリストに含まれていない場合に適用されます。たとえば、新しいドメインが Microsoft 365 アカウントに追加されているが、Secure Email Threat Defense にインポートされていない場合などです。	[選択（Checked）] または [選択解除（Unchecked）]	**選択解除（Unchecked）**。[読み取り/書き込み（Read/Write）] モードをオンにする場合は、このチェックボックスをオンにしてすべての内部電子メールに自動修復が適用されるようにします。

ゲートウェイを使用している場合のポリシー設定

Cisco E メール セキュリティ アプライアンスまたは同様のゲートウェイを配置している場合は、次のポリシー設定の使用を検討してください。

表 2　　ゲートウェイで推奨されるポリシー設定

設定名	推奨される選択
Cisco Secure Email Gateway（SEG）	[SEGがあります（SEG is present）]。ヘッダーを表示します
Message Analysis	[スパムおよびグレイメール（Spam and Graymail）] を [オフ（Off）]
Remediation Actions	[脅威（Threats）] - [隔離に移動（Move to Quarantine）]

Cisco Secure Email Gateway（SEG）が存在することと、受信ジャーナルでの SEG の識別に使用できるヘッダーを示すことにより、Secure Email Threat Defense でメッセージの真の発信者を特定できるようにすることが重要です。この設定を行わないと、SEG から送信されたすべてのメッセージが表示され、誤検出が発生する可能性があります。

Cisco Secure Email Cloud Gateway（旧 CES）または Cisco Secure Email Gateway（旧 ESA）のヘッダーの確認または設定については、
https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox
を参照してください。

また、メッセージの送信元に Microsoft 365 を使用している場合は、ジャーナルが Microsoft 365 から Secure Email Threat Defense に直接送信されるように、アプライアンスをバイパスすることを推奨します。バイパスするには、Secure Email Threat Defense の設定（11 ページ）で説明されているように、Microsoft 365 にコネクタを追加します。

メッセージの送信元の切り替え

メッセージの送信元を変更するには、**[ポリシー(Policy)]** ページに移動します。

1. 新しいメッセージの送信元に対応するラジオボタンを選択します。
2. メッセージの送信元を切り替えることを示す通知が表示されます。[Continue] をクリックします。
3. [メッセージの送信元の切り替え(Switch Message Source)] ダイアログが表示されます。Cisco Secure Email Threat Defense へのメッセージの送信を停止するには、以前のメッセージの送信元を設定する必要があります。この設定方法の詳細については、Cisco Secure Email Threat Defense ジャーナルルールの削除(69 ページ)またはメッセージの送信を停止するようにゲートウェイを構成する(70 ページ)を参照してください。
4. 以前の送信元でジャーナルまたはメッセージの送信を停止したことを示すチェックボックスをオンにしてから、[次へ(Next)] をクリックします。
5. ダイアログに表示されるメッセージ受信アドレスまたはジャーナルアドレスを使用して、新しいメッセージの送信元を設定します。各タイプのメッセージの送信元を設定する手順については、メッセージの送信元の設定(12 ページ)で詳しく説明します。

メッセージ

[メッセージ(Messages)] ページにはメッセージと検索結果が表示され、侵害の可能性を調べることができます。1 ページあたり最大 100 件のメッセージを表示できます。

[メッセージ(Messages)] ページのアイコン

次の表に、[メッセージ(Messages)] ページで使用されるアイコンとその意味を示します。

表 1　　[メッセージ(Messages)] ページのアイコン

アイコン	名前	説明
	リンク	メッセージにリンクが含まれています。
	添付ファイル	メッセージに添付ファイルが含まれています
	手動で修正または手動で再分類	メッセージが手動で修正または再分類されました。メッセージが修正された場合は [アクション(Action)] の横に、メッセージが再分類された場合は [判定(Verdict)] の横にアイコンが表示されます。
	レトロスペクティブな判定	レトロスペクティブな判定が適用されました。レトロスペクティブな判定は、メッセージが Secure Email Threat Defense によって最初にスキャンされた後に適用されたものです。
	許可	メッセージが、指定された項目(許可リスト、MS 許可リスト、または安全な送信者)に基づいて許可されました。
	判定のオーバーライド	判定が、判定のオーバーライド メッセージ ルールに基づいてオーバーライドされました。
	バイパス分析	バイパス分析メッセージルールにより、メッセージが分析されませんでした。ルールのタイプ(セキュリティメールボックスまたはフィッシングテスト)が指定されています。
	BEC	メッセージが手動で、または自動修復によってビジネスメール詐欺(BEC)としてマークされました。
	詐欺	メッセージが手動で、または自動修復によって詐欺としてマークされました。

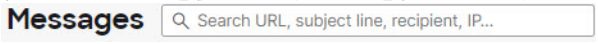
表 1　　[メッセージ(Messages)] ページのアイコン

アイコン	名前	説明
	フィッシング	メッセージは、手動または自動修復によってフィッシングとしてマークされています。
	悪意あり	メッセージは、手動または自動修復によって悪意のあるものとしてマークされています。
	スパム	メッセージが手動または自動修復によってスパムとしてマークされました。
	グレイメール	メッセージがグレイメールとしてマークされています。グレイメールは、マーケティング、ソーシャル、またはジャンクと判断されたメールです。
	ニュートラル	メッセージがニュートラルとしてマークされています。
	着信	O365 テナント外から受信したメール。
	内部	O365 テナント内で送信されたメール。
	発信	O365 テナント外の受信者に送信されたメール。

検索およびフィルタ

カレンダーコントロールを使用して、定義された期間(直近の日、週、または月)のデータや、過去 90 日以内のカスタムタイムフレームのデータを表示します。

検索フィールドを使用して、文字列を検索したり、ハッシュや URL などの注目する指標を検索します。

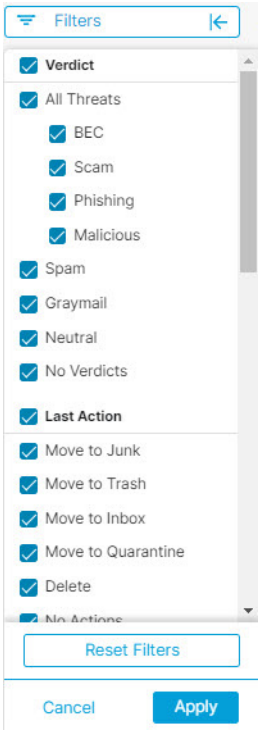


[フィルタ(Filter)] パネル

フィルタパネルを使用して検索を絞り込みます。たとえば、特定の送信者から送信されたすべてのメール、特定の判定のメール、添付ファイルやリンクがあるメール、再分類されたメール、[迷惑メール(Junk)] に移動されたメールなどを表示できます。

1. 矢印をクリックして、フィルタパネルを展開します。

2. 選択を行い、[適用(Apply)] をクリックします。[判定(Verdict)] の少なくとも 1 つの項目を選択する必要があることに注意してください。

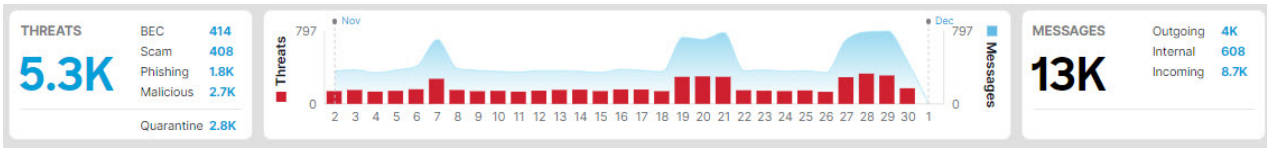


フィルタをデフォルトにリセットには、[フィルタのリセット(Reset Filters)] ボタンを使用します。

メッセージグラフとクイックフィルタ

[メッセージ(Messages)] ページの上部にあるメッセージグラフとクイックフィルタは、メッセージトラフィックのグラフィカルビューを提供します。このグラフを使用して、メッセージをすばやくフィルタ処理します。グラフには、次のものが含まれています。

- 脅威とカテゴリのブレークアウトにより、合計を表示し、脅威を簡単にフィルタ処理します。
- 隔離された項目をフィルタ処理するために使用できる [隔離(Quarantine)] の合計
- 方向ですばやくフィルタ処理するために使用できる [メッセージの方向(Message Direction)] の合計



判定

Cisco Secure Email Threat Defense は、次の脅威判定をメッセージに適用します。

- [BEC]:ビジネスメール詐欺(BEC)は、ソーシャルエンジニアリングと侵入技術を使用して組織に経済的損害を与える高度な詐欺です。
- [詐欺(Scam)]:詐欺は、宝くじ詐欺や強要詐欺などの手法を使用して、個人に経済的損害を与えることに焦点を当てています。

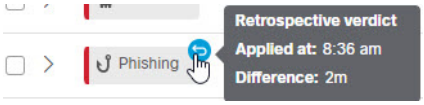
- [フィッシング(Fishing)]:これらのメッセージは、ユーザー名、パスワード、クレジットカード番号などの機密情報を取得しようとして、正規のサービスを不正にコピーまたは模倣したとして有罪判決を受けています。
- [悪意のある(Malicious)]:これらのメッセージは、悪意のあるソフトウェアの配信または拡散を含む、提供する、または支援するとして有罪判決を受けています。

レトロスペクティブな判定

レトロスペクティブな判定は、メッセージが Secure Email Threat Defense によって最初にスキャンされた後のある時点でメッセージに適用されたものです。

Secure Email Threat Defense のレトロスペクティブな判定は、他のシスコのセキュリティ製品とは若干異なります。Secure Email Threat Defense はインラインメールプロセッサではありませんが、メッセージの初期分析を完了するための固定の時間範囲があります。Talos のディープ URL 分析など、分析時間が長い新しいコンテンツエンジンは、レトロスペクティブな判定として扱われます。判定が遅れると、修復も遅れます。したがって、Secure Email Threat Defense はこれらの判定を明確にタグ付けします。

レトロスペクティブな判定は、[メッセージ(Messages)] ページの [判定(Verdict)] の隣に青いアイコンで示されます。アイコンにカーソルを合わせると、レトロスペクティブな判定が適用された時刻と、メッセージを受信した時刻と判定が適用された時刻の差異が表示されます。



レトロスペクティブな判定の電子メール通知

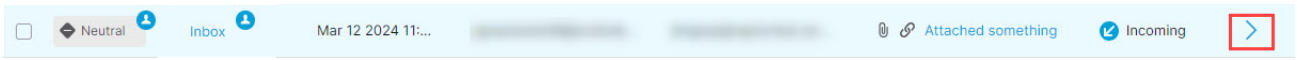
レトロスペクティブな判定の電子メール通知をオンまたはオフにするには、次の手順を実行します。

1. **[管理(Administration)]** > **[ビジネス(Business)]** の順に選択します。
2. [初期設定(Preferences)] で、[レトロスペクティブな判定の通知を送信(Send Notifications for Retrospective Verdicts)] を選択または選択解除します。

このチェックボックスがオンの場合、レトロスペクティブな判定の電子メール通知が通知用に指定された電子メールアドレスに送信されます。これらの通知はデフォルトでオンになっています。

メッセージレポート

メッセージレポートを使用すると、メッセージに関する詳細を調査できます。**>** アイコンを選択するか、メッセージ行の任意の場所をクリックして、そのメッセージのレポートにアクセスします。

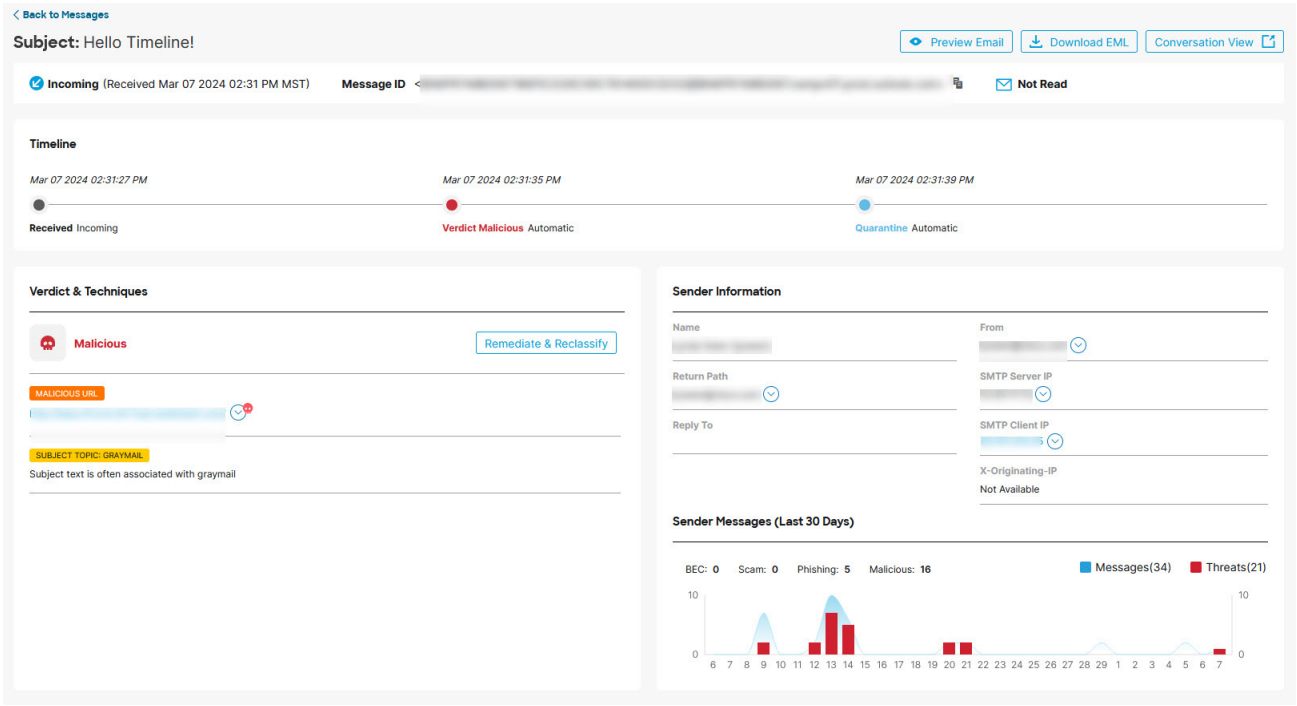


メッセージレポートには、次のようなメッセージに関する詳細が表示されます。

- メッセージの方向、Microsoft Message ID、および修復時にメッセージが開封されたかどうか
- タイムライン
- 判定と手法
- 送信者情報
- 送信者メッセージ
- 受信者、エンベロープ受信者、メールボックスなどの受信者情報
- リンク

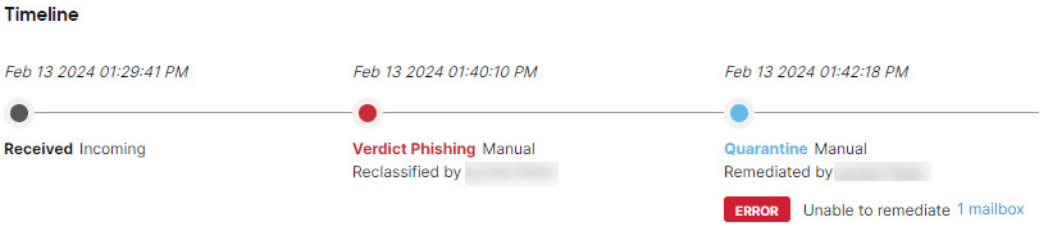
- 添付ファイル
- 電子メールのプレビュー

メッセージレポートでは、カンバセーションビューや EML ダウンロードにもアクセスできます。



タイムライン

メッセージのタイムラインは、メッセージレポートに表示されます。



タイムラインには次の情報が表示されます。

- **[受信(Received)]**: メッセージを受信した時刻、およびメッセージの方向に関する詳細
- **[ルール(Rule)]**: 適用されたメッセージルールに関する情報
- **[判定(Verdict)]**: 示されたまたは適用された判定に関する情報と、アクションの実行者
- **[アクション(Action)]**: メッセージに対して実行されたアクションに関する情報と、アクションの実行者次の機能が含まれています。
  - メッセージの移動場所と移動方法
  - メッセージの修復エラーに関する情報と、エラーが発生したメールボックス

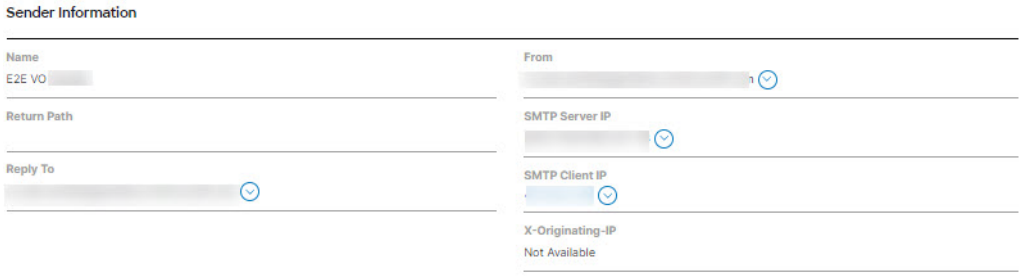
判定と手法

[判定と手法(Verdict and Techniques)] パネルには、メッセージに適用された判定と、検出された手法で判定に寄与した可能性があるものが視覚的に表示されます。手法は、その重大度を示すために色分けされています。悪意のあるファイルの名前/SHA256 および URL は、動的に表示されます(動的な表示が可能な場合)。動的テキストが使用できない場合は、静的な説明が表示されます。

このパネルから直接メッセージを修復または再分類できます。[修復と再分類(Remediate and Reclassify)] ボタンをクリックし、メッセージの移動と再分類(29 ページ) に記載されている手順に従います。

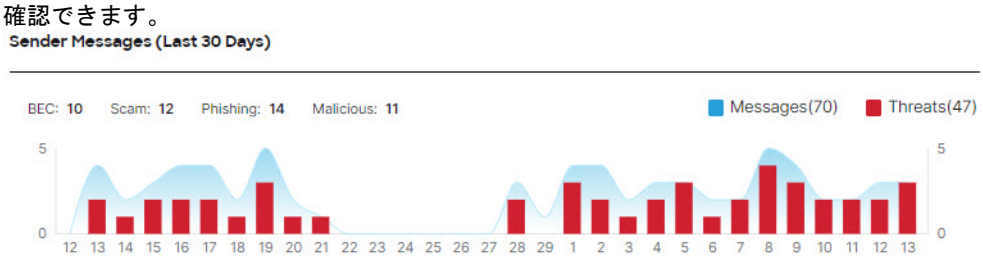
送信者情報

[送信者情報(Sender Information)] パネルには、名前、電子メールアドレス、リターンパス、返信先、SMTP サーバーとクライアントの IP、X-Originating IP など、メッセージの送信者に関する既知の情報が表示されます。



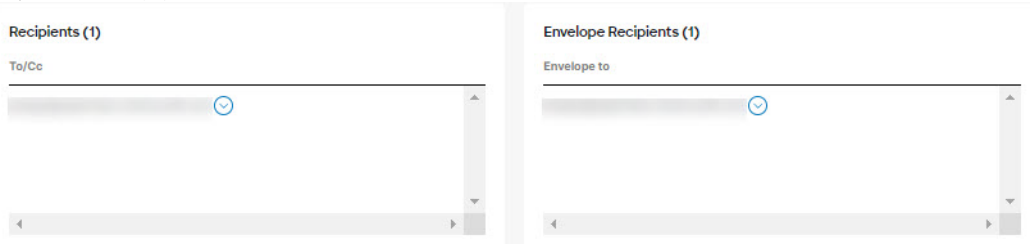
送信者メッセージ

[送信者メッセージ(Sender Messages)] グラフには、過去 30 日間にメッセージの送信者が送信したメッセージの合計数と脅威メッセージの合計数が表示されます。これにより、ユーザーからの脅威メッセージのパターンがあるかどうかをすばやく確認できます。



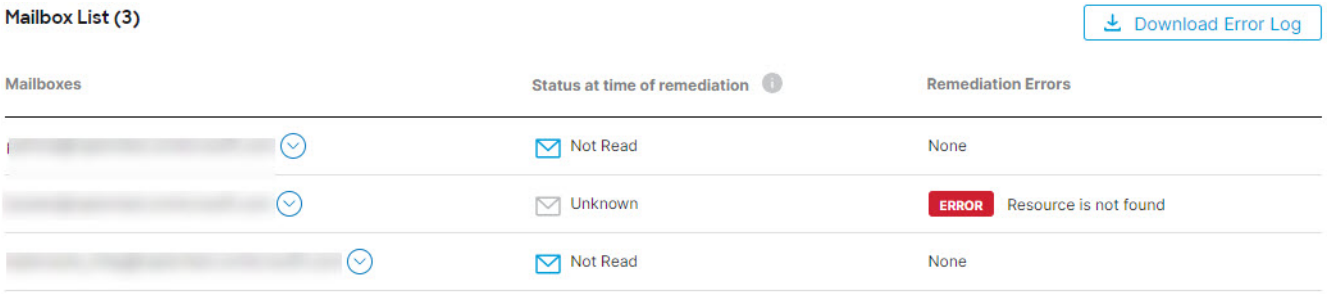
受信者情報

[受信者(Recipients)] パネルと [エンベロープ受信者(Envelope Recipients)] パネルには、メッセージの送信先に関する情報が表示されます。



メールボックスリスト

メールボックスリストには、着信メッセージと内部メッセージを受信したエンドユーザーのメールボックスのリストが表示されます。このリストには、メッセージが最後の修復アクションの前に開封されたかどうかと、メッセージの修復エラーも表示されます。修復エラーは、システムが修復を試みる前にユーザーがメッセージを削除または移動した場合に発生する可能性があります。

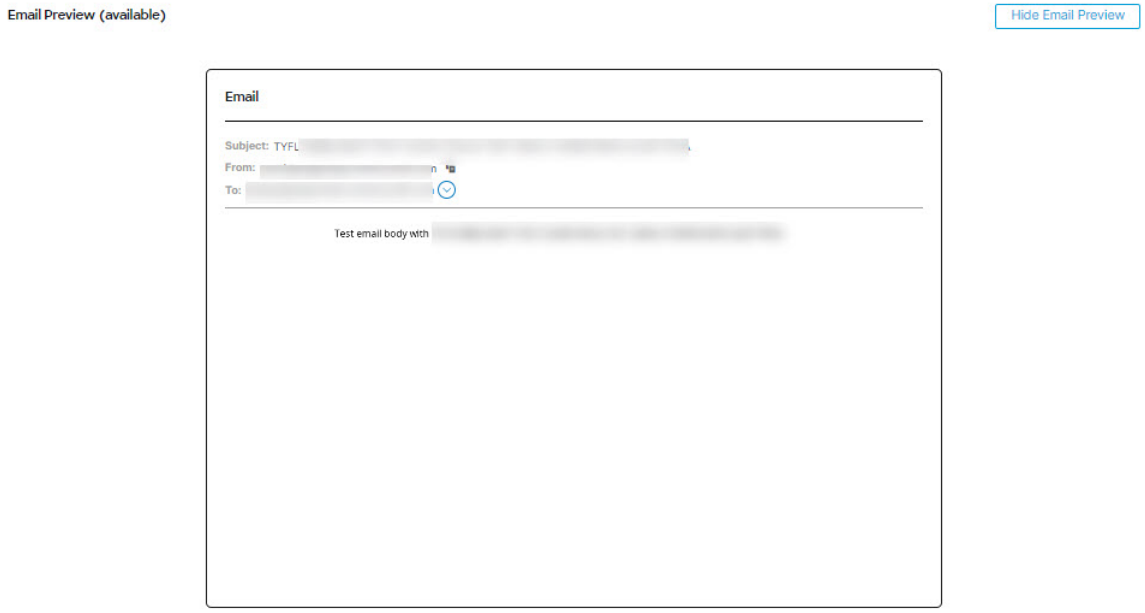


リンクと添付ファイル

[リンクと添付ファイル(Links and Attachment)] パネルには、メッセージ内で見つかったリンクと添付ファイルに関する情報が表示されます。

電子メールのプレビュー

電子メールプレビューを使用すると、ネットワーク管理者および管理者ユーザーは、EML ファイルをダウンロードすることなく、エンドユーザーに表示されるメッセージを要求して表示できます。メッセージはイメージとして表示されます。**[電子メールプレビューを開く(Open Email Preview)]** ボタンをクリックして、プレビューを表示します。



ユーザーがメッセージをプレビューすると、監査ログレコードが作成されます。監査ログは、**[管理(Administration)]** > **[ビジネス (Business)]** > **[初期設定(Preferences)]** からダウンロードできます。

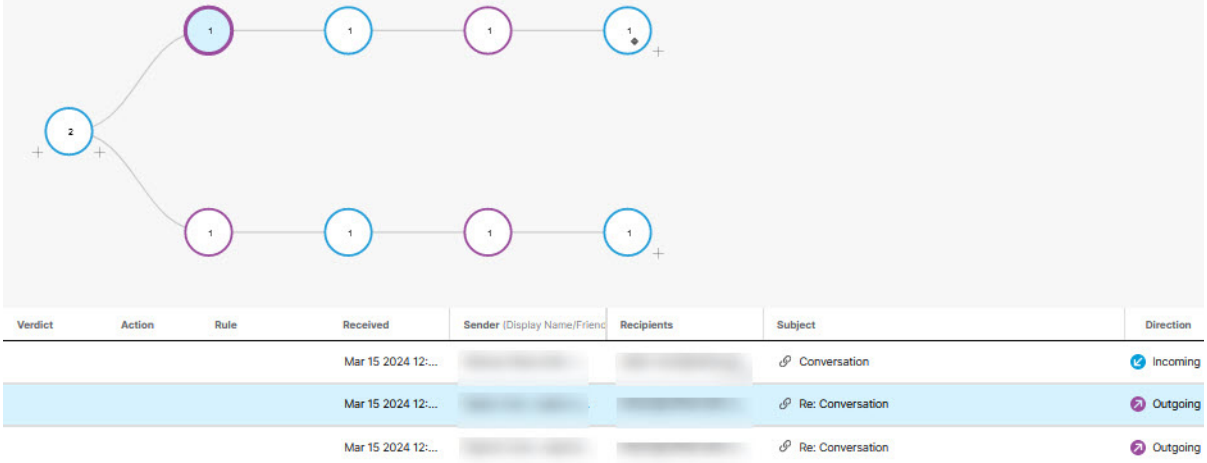
カンバセーションビュー

カンバセーションビューでは、カンバセーションの全体ビューが表示されます。カンバセーションビューを使用して、カンバセーション内のメッセージを追跡し、メールフローを完全に把握します。これは、脅威の発生源と組織内で拡散する方法を判断するのに役立ちます。

メッセージレポートで、ページの右上にある [カンバセーションビュー(Conversation View)] ボタンをクリックして、特定の電子メールに関連するメッセージを表示します。

[+] アイコンをクリックしてカンバセーションのノードを展開すると、カンバセーションの前後のメッセージを確認できます。展開されたノードは、ノードの下に表示されるメッセージグリッドに追加されます。ノードとメッセージは、方向(着信、発信、または内部)を示すために色分けされています。

ノード円内の数字は、メッセージの送信先アドレス数を示します。ノード内のアイコンは、脅威が検出されたかどうか、または判定が適用されたかどうかを示します。ノードを選択すると、対応するメッセージがグリッド内で強調表示されます。



XDR ピボットメニュー

Cisco Secure Email Threat Defense ビジネスが Cisco XDR と統合されている場合、メッセージレポート内から XDR ピボットメニューにアクセスできます。XDR との統合の詳細については、XDR（63 ページ）を参照してください。

メッセージの移動と再分類

誤って分類されたと思われるメッセージを移動または再分類するには、[メッセージ（Messages）] ページを使用します。1 ページに表示されるメッセージ数を変更することで、一度に最大 100 件のメッセージを移動または再分類できます。[メッセージレポート（Message Report）] ページの [判定と手法（Verdict and Techniques）] パネルから直接メッセージを移動および再分類することもできます。

修復と再分類 API を使用して、メッセージを移動および再分類することもできます。詳細については、API ガイド（https://developer.cisco.com/docs/message-search-api/）を参照してください。

注：再分類は、選択したメッセージの判定にのみ影響します。これは、選択した送信者からの今後のメッセージに対する、またはメッセージの内容に基づくアクションの変更を示すものではありません。メッセージは、Cisco Talos による確認のためにキューに入れられます。Talos は、今後の分類に影響を与えるためにこのフィードバックを使用する場合があります。誤検出メッセージについては、判定のオーバーライドルール（58 ページ）の追加を検討してください。

ハイブリッド Exchange アカウントについて

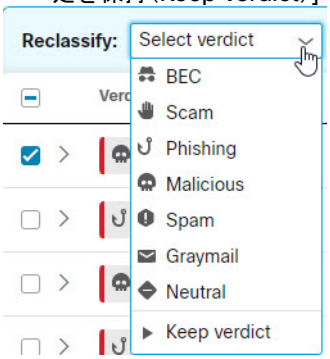
Secure Email Threat Defense は、Exchange Online（O365）に存在するメールボックス上でのみ動作します。メールボックスをオンプレミスの Exchange から Exchange Online（O365）に移行中の場合、修復（移動または削除）は、Exchange Online（O365）にあるメールボックスに対してのみ機能します。オンプレミスの Exchange メールボックスの修復が失敗したことは通知されません。

読み取り修復モード

読み取りモードでは、メッセージの再分類（異なる判定の適用）が可能です。

1. 再分類するメッセージを選択します。

2. ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] を選択できます。



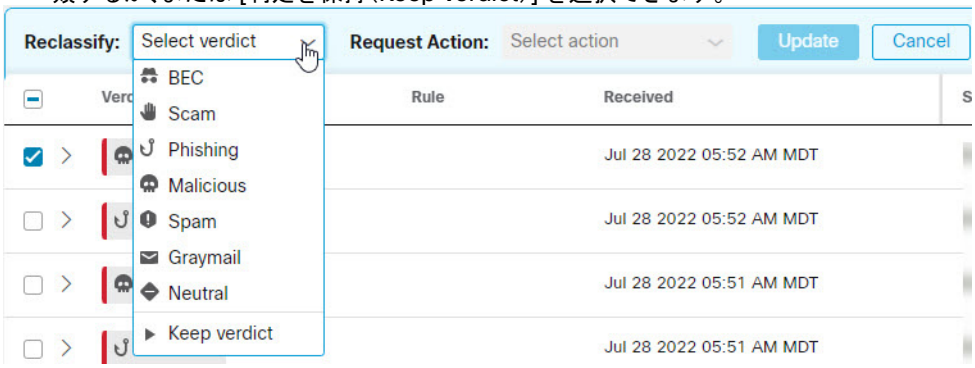
3. 新しい分類を適用するには、[更新(Update)] をクリックします。

読み取り/書き込み修復モード

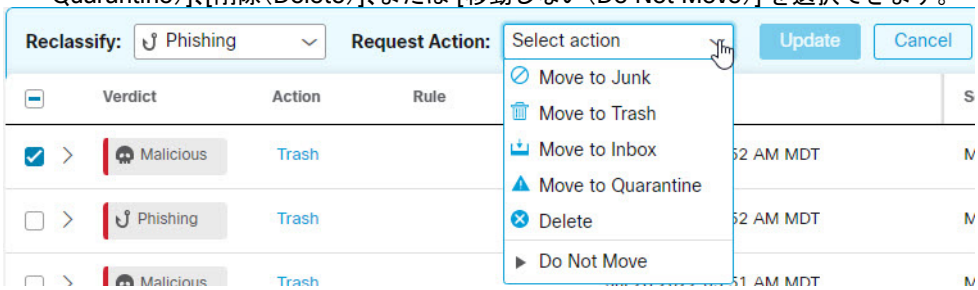
読み取り/書き込み修復モードでは、疑わしいメッセージをユーザーの受信トレイから迷惑メールまたはゴミ箱に移動するか、ユーザーがアクセスできない検疫フォルダに移動できます。同様に、迷惑メール、ゴミ箱、または検疫に移動されたメッセージが疑わしくないと判断した場合は、そのメッセージをユーザーの受信トレイに戻すことができます。メッセージを完全に削除することもできます。このプロセスでは、メッセージを再分類(異なる判定を適用)することもできます。

1. 移動または再分類するメッセージを選択します。

2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)]に再分類するか、または [判定を保持(Keep verdict)] を選択できます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューからアクションを選択します。[迷惑メールに移動(Move to Junk)]、[ゴミ箱に移動(Move to Trash)]、[受信トレイに移動(Move to Inbox)]、[隔離に移動(Move to Quarantine)]、[削除(Delete)]、または [移動しない(Do Not Move)] を選択できます。



4. [更新(Refresh)] をクリックして新しい分類を適用し、メッセージに対してアクションを実行します。

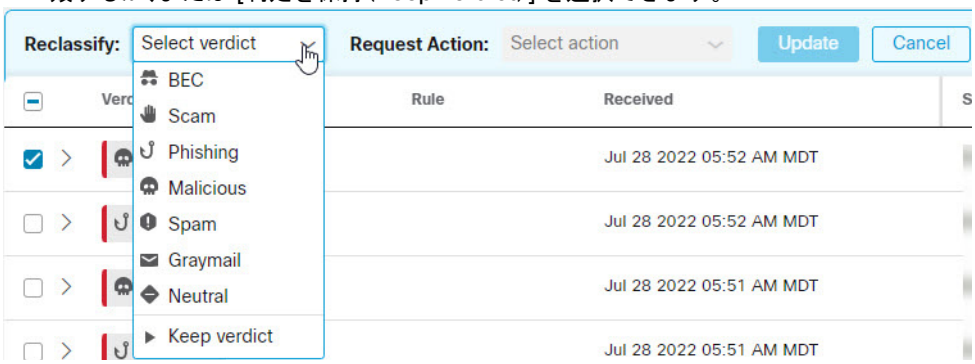
メッセージが移動された場合は、[最後のアクション(Last Action)] 列に示されます。

注: 発信メッセージと内部メッセージの場合、[受信トレイに移動(Move to Inbox)] アクションは、メッセージを受信トレイではなく、メッセージの最初の送信者の [送信済み(Sent)] フォルダに移動します。

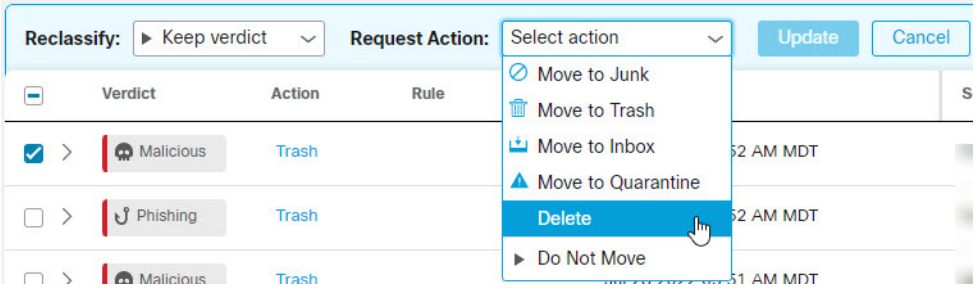
メッセージを削除する

スーパー管理者および管理ユーザーは、再分類/修正ワークフローの削除アクションを使用して、メールボックスからメッセージを完全に削除できます。削除されたメッセージは、**recoverableitemspurges** フォルダに移動されます。ユーザーはこのフォルダにアクセスできず、Secure Email Threat Defense では削除されたメッセージを受信トレイに復元できません。

1. 削除するメッセージを選択します。
2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] を選択できます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューから [削除(Delete)] を選択します。



4. [更新(Update)] をクリックしてメッセージを削除します。
5. [削除の確認(Confirm Deletion)] ダイアログに、メッセージは復元できないことが表示され、続行するかどうか確認されます。続行するには、[削除(Delete)] をクリックします。

[最後のアクション(Last Action)] 列に削除が表示されます。

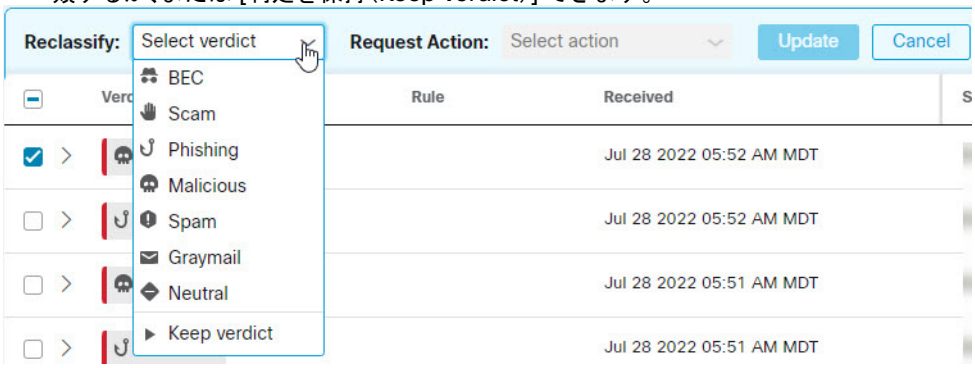
メッセージの隔離

検疫フォルダはメールボックスごとに自動的に作成され、Outlook ユーザーには表示されません。シークレットフォルダ名は、**[管理(Administration)]** > **[ビジネス(Business)]** ページで、ネットワーク管理者および管理者ユーザーに表示されます。Outlook では、検疫フォルダ内のメッセージは、削除済み項目の消去設定に従って自動的に消去されます。Secure Email Threat Defense では、検疫フォルダから消去されたメッセージをユーザーの受信トレイに復元することはできません。

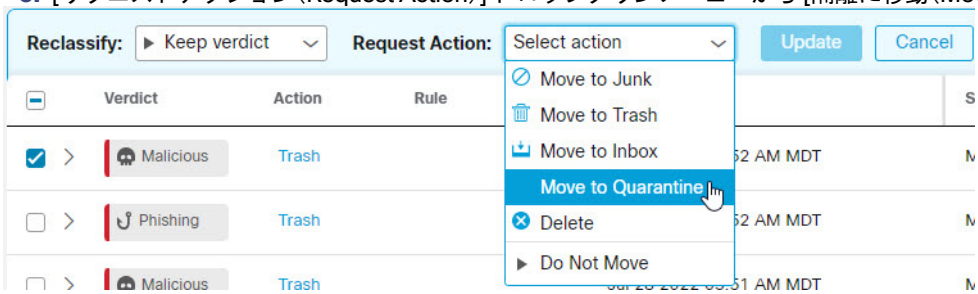
メッセージを手動で隔離に移動するには、次の手順を実行します。

1. 隔離に移動するメッセージを選択します。

2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] できます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューから [隔離に移動(Move to Quarantine)] を選択します。



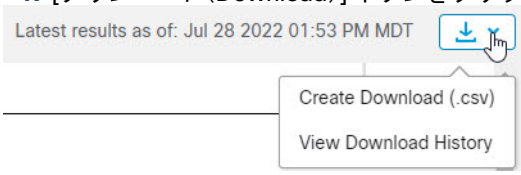
4. [更新(Update)] をクリックして、メッセージを隔離します。

[隔離に移動(Move to Quarantine)] は、[最後のアクション(Last Action)] 列に表示されます。

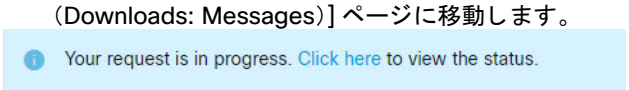
検索結果のダウンロード

検索結果のメッセージに関するデータの CSV ファイルをダウンロードできます。ダウンロードは 10,000 メッセージに制限されています。データをダウンロードするには、次の手順を実行します。

1. [ダウンロード(Download)] ボタンをクリックし、[ダウンロードの作成(.csv)(Create Download (.csv))] を選択します。



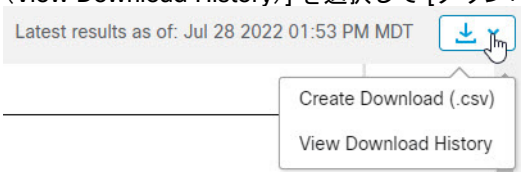
2. 要求が進行中であることを示すバナーが表示されます。テキストをクリックして、[ダウンロード:メッセージ(Downloads: Messages)] ページに移動します。



3. ダウンロードの準備ができたら、[アクション(Actions)] 列の [ダウンロード(Download)] アイコンをクリックしてファイルをダウンロードします。

ダウンロード履歴

ダウンロード履歴は 90 日間保持されます。[ダウンロード（Download）] ボタンをクリックし、[ダウンロード履歴の表示（View Download History）] を選択して [ダウンロード：メッセージ（Download: Messages）] ページに移動します。



このページには、日付範囲、ダウンロードを要求したユーザー、ダウンロードが開始された日付、およびステータスが表示されます。[アクション（Actions）] 列の [ダウンロード（Download）] アイコンを選択して、ファイルをダウンロードします。

検索結果のダウンロード

ダウンロード

画面右上隅の [ダウンロード（Downloads）] メニューからアクセスできるページでは、以下を作成および管理できます。

- 検索結果メッセージデータ CSV
- 修復エラーログ SCV
- EML ダウンロード要求

メッセージ

セキュリティ、コンプライアンス、分析、または管理の目的で電子メールデータを活用する必要がある場合は、検索結果のメッセージデータを CSV 形式でダウンロードできます。CSV では、次の属性によってデータが整理されています。

- メッセージ ID
- 判定（BEC、詐欺、フィッシング、悪意がある、スパム、グレイメール、ニュートラル、判定なし）
- 最後のアクション（隔離、ジャンクメール、ごみ箱、受信トレイ）
- 修復方法（自動、手動、API）
- レトロスペクティブな判定（TRUE または FALSE）
- 受信（日付と時刻）
- 表示名
- 送信者
- 返信先
- リターンパス
- エンベロープ送信者
- 送信側 IP（Sending IP）
- 受信側 IP（Receiving IP）
- X Originating IP
- 受信者
- サブジェクト
- 添付ファイル
- URL
- 方向（着信、発信、内部）
- ルール名（Rule Name）

- ルール タイプ
- ソース
- 配信先
- エンベロープ送信先

メッセージデータは次の 2 つの方法でダウンロードできます。

- 検索結果のダウンロード（32 ページ）で説明されているように、[メッセージ（Messages）] ページから。特定のフィルタリングされたデータまたは長期間のデータをダウンロードする場合は、このオプションを使用します。現在の検索結果とフィルタ結果にあるメッセージのデータの CSV ファイルを作成します。
- 以下で説明されているように、[ダウンロード（Downloads）] > [メッセージ（CSV）（Messages (CSV)）] タブから。これは、過去 24 時間、過去 7 日間、特定の日や週など、特定の期間のすべてのメッセージデータをダウンロードする場合に便利です。

[ダウンロード（Downloads）] ページからメッセージデータの CSV を作成してダウンロードするには、次の手順を実行します。

1. [ダウンロード（Downloads）] > [メッセージ（CSV）（Messages (CSV)）] を選択します。
2. [CSVを作成（Create CSV）] をクリックします。
3. 表示されるダイアログで、ダウンロードを作成する日付範囲を選択し、[CSVを作成（Create CSV）] をクリックします。
4. ダウンロードの準備ができたら、[アクション（Actions）] 列の [ダウンロード（Download）] アイコンをクリックしてファイルをダウンロードします。

EML ダウンロード

スーパー管理者および管理者ユーザーは、展開されたメッセージビューから EML ダウンロードを要求できます。サイズの小さいダウンロードはすぐに実行されます。サイズの大きいダウンロードは、ダウンロードの完了と 7 日間経過のいずれか早い方まで、[ダウンロード（Downloads）] ページから利用できます。[ダウンロード（Downloads）] ページから複数のファイルを一度にダウンロードできます。**[ダウンロード（Downloads）]** > **[EMLのダウンロード（Download EML）]** から直接 [ダウンロード（Downloads）] ページにアクセスできます。

EML ファイルを要求してダウンロードするには、次の手順に従います。

1. メッセージレポートで、[EMLダウンロードの要求（Request EML Download）] ボタンをクリックします。小さいメッセージはすぐにダウンロードされます。
2. 時間のかかるダウンロードについては、要求が進行中であることを示すバナーが表示されます。テキストをクリックして、[ダウンロード：EMLダウンロード（Downloads: Download EML）] ページに移動します。
3. ダウンロードの準備ができたら、[アクション（Actions）] 列の [ダウンロード（Download）] アイコンをクリックしてファイルをダウンロードします。

修復エラーログ

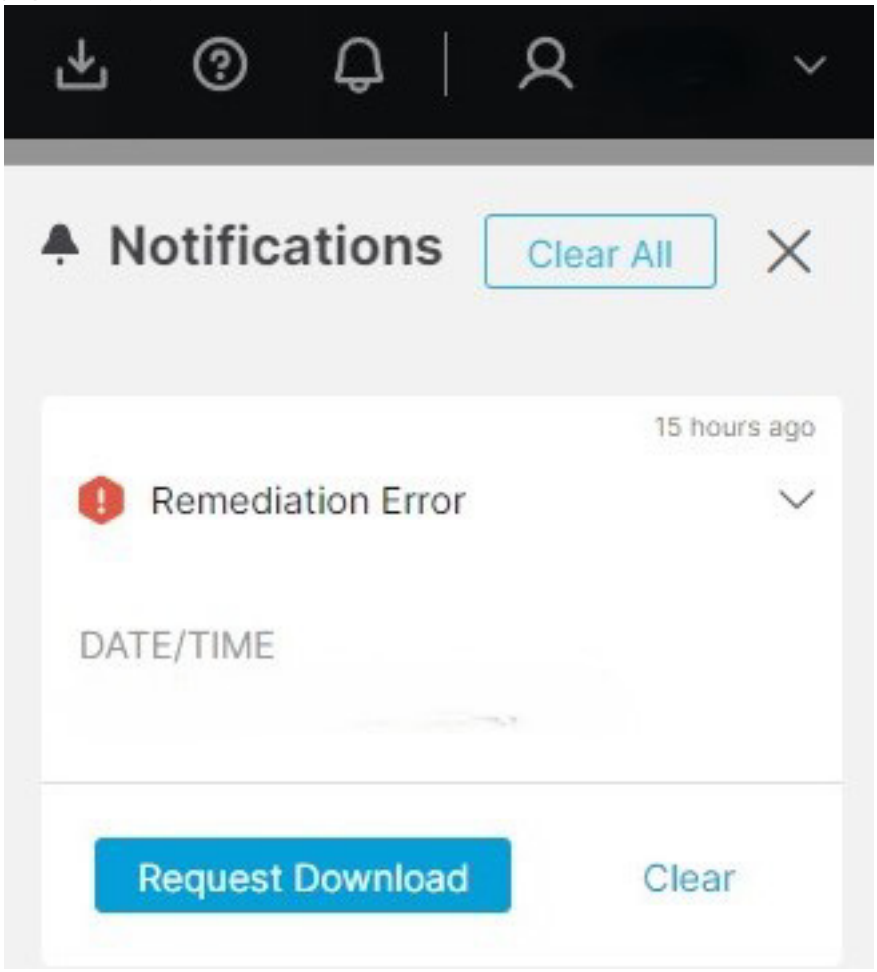
修復エラーが発生すると、[通知（Notifications）]（ベルアイコン）メニューの下に通知が表示されます。修復エラーログを使用すると、個々のメールボックスの修復失敗を調査できます。たとえば、メールボックスの所有者によってメッセージがすでに削除されている場合、Move to Trash リクエストは失敗する可能性があります。修復エラーログには、リソースが見つからないことが示されます。

修復エラーログは、次の属性でデータを整理した CSV ファイルです。

- 要求 ID
- Timestamp

- ユーザーの電子メール ID
- フォルダ要求
- メールボックス（Mailbox）
- アクション タイプ
- 理由

通知を展開して [ダウンロードの要求（Request Download）] をクリックすると、通知から直接エラーログのダウンロードを要求できます。



または、次の手順を実行して、修復エラーログを作成しダウンロードします。

1. **[ダウンロード（Downloads）]** > **[修復エラーログ（Remediation Error Log）]** を選択します。
2. [CSVを作成（Create CSV）] をクリックします。
3. 表示されるダイアログで、ダウンロードを作成する日付範囲を選択し、[CSVを作成（Create CSV）] をクリックします。
4. ダウンロードの準備ができたら、[アクション（Actions）] 列の [ダウンロード（Download）] アイコンをクリックしてファイルをダウンロードします。

修復エラーログ

インサイト

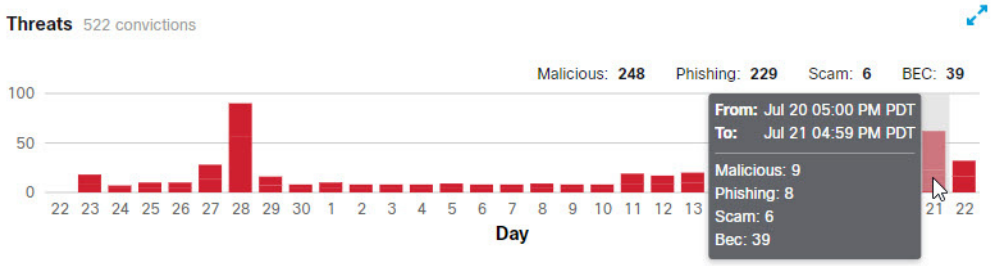
トレンド

[トレンド(Trends)] ページには、電子メールデータに関するグラフィカル情報が表示されます。トレンドを表示するには、[インサイト(Insights)] > [トレンド(Trends)] を選択します。

- カレンダーコントロールを使用して、特定の日、週、または月のデータを表示します。
- グラフ内の注目するデータをクリックすると、[メッセージ(Messages)] ページのデータの詳細に移動します。
- 凡例項目をクリックして、[メッセージ(Messages)] ページの関連データに移動します。たとえば、[着信(Incoming)] をクリックすると、チャートに現在表示されているすべての着信メッセージが表示されます。
- ダウンロード ボタンをクリックして、トレンドデータをダウンロードします。結果は、次を含む CSV ファイルとしてエクスポートされます。
  - 過去 24 時間または特定の日を表示している場合、過去 90 日間のデータの 1 時間ごとのロールアップ
  - 過去 30 日間のデータを表示している場合、過去 90 日間のデータの 24 時間のロールアップ
- 印刷 ボタンをクリックして、[インサイト(Insights)] のチャートを印刷するか PDF として保存します。

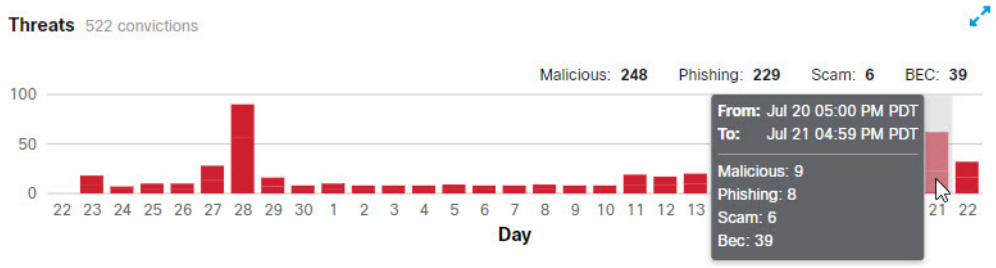
タイムゾーンについて

特定の [日(Day)] チャートの各棒は、1 時間分のデータを示します。これらのチャートは、ブラウザのローカルタイムゾーンに基づいています。



特定の [週(Week)] チャートまたは [月(Month)] チャートの各棒は、1 日分(24 時間)のデータを示します。日は UTC 00:00 ～午後 11:59 を基準とし、ブラウザのローカル時間に変換されます。

たとえば、太平洋夏時間（PDT）で UTC 07:00 の場合、[月（Month）] チャートの棒には、7 月 20 日の午後 5 時から 7 月 21 日の午後 4 時 59 分までのデータが表示されます。

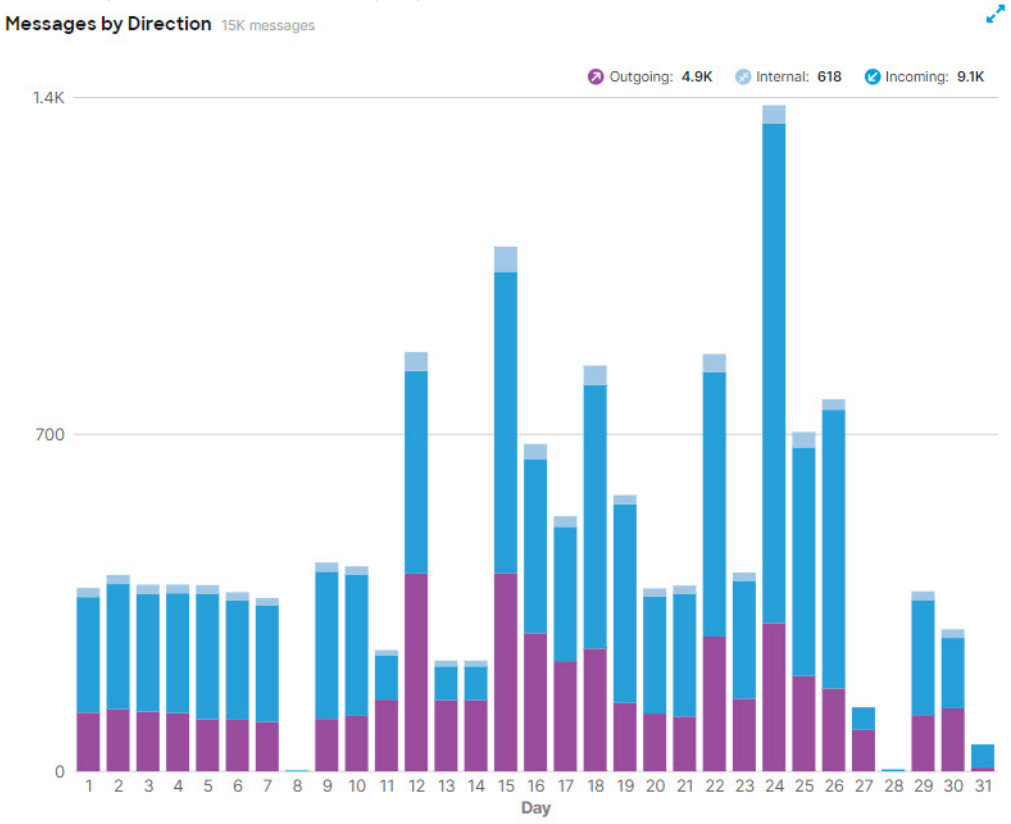


宛先別メッセージ

[宛先別メッセージ（Messages by Direction）] グラフには、電子メールトラフィックの合計が表示されます。メールは、次のカテゴリに分かれています。

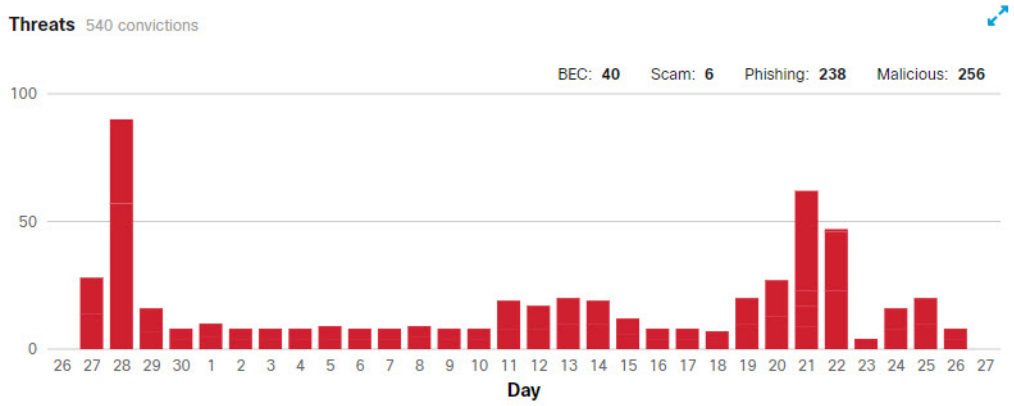
- [発信（Outgoing）]：0365 テナント外の受信者に送信されたメール
- [内部（Internal）]：O365 テナント内で送信されたメール
- [着信（Incoming）]：0365 テナント外から受信したメール

凡例には、各カテゴリのメッセージ数が表示されます。



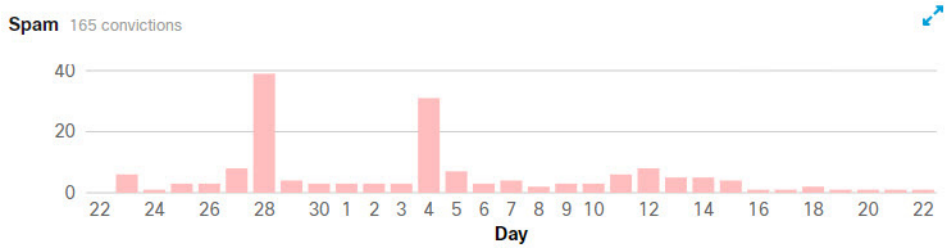
脅威

[脅威(Threats)] グラフには、脅威と判定されたメッセージのスナップショットが表示されます。これには BEC、詐欺、フィッシング、および悪意のあるものが含まれます。凡例には、各カテゴリのメッセージ数が表示されます。データをクリックして、[メッセージ(Messages)] ページに移動します。



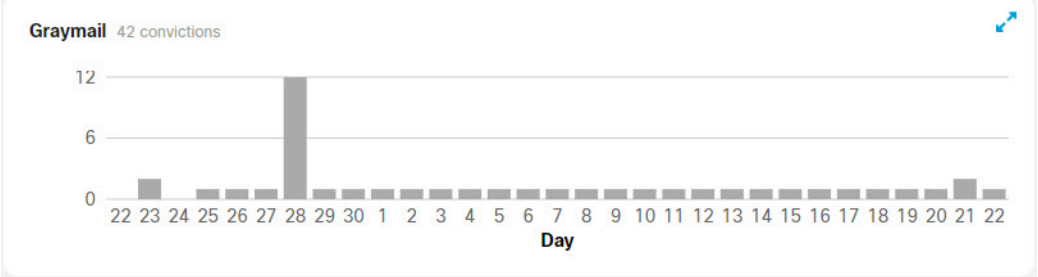
スパム

[スパム(Spam)] グラフには、スパムと判定されたメッセージのスナップショットが表示されます。凡例には、スパムと判定されたメッセージの総数が表示されます。



グレイメール

[グレイメール(Graymail)] グラフには、グレイメールと判定されたメッセージのスナップショットが表示されます。凡例には、グレイメールと判定されたメッセージの合計数が表示されます。

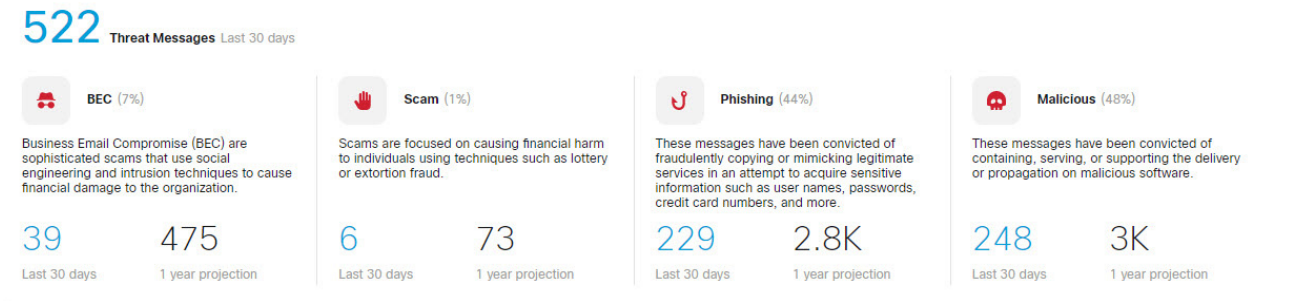


影響レポート

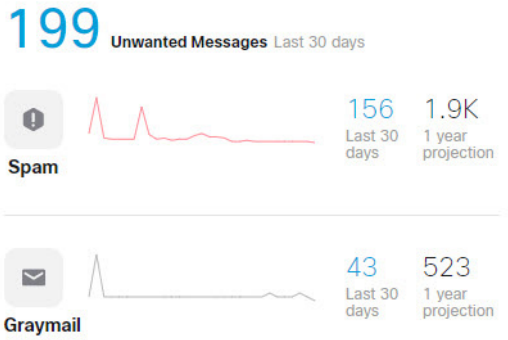
[影響レポート (Impact Report)] には、過去 30 日間に Cisco Secure Email Threat Defense がもたらしたメリットが表示されます。このレポートを表示するには、[インサイト (Insights)] > [影響レポート (Impact Report)] を選択します。レポート内の注目するデータをクリックすると、[メッセージ(Messages)] ページのデータの詳細に移動します。

表示されるデータは次のとおりです。

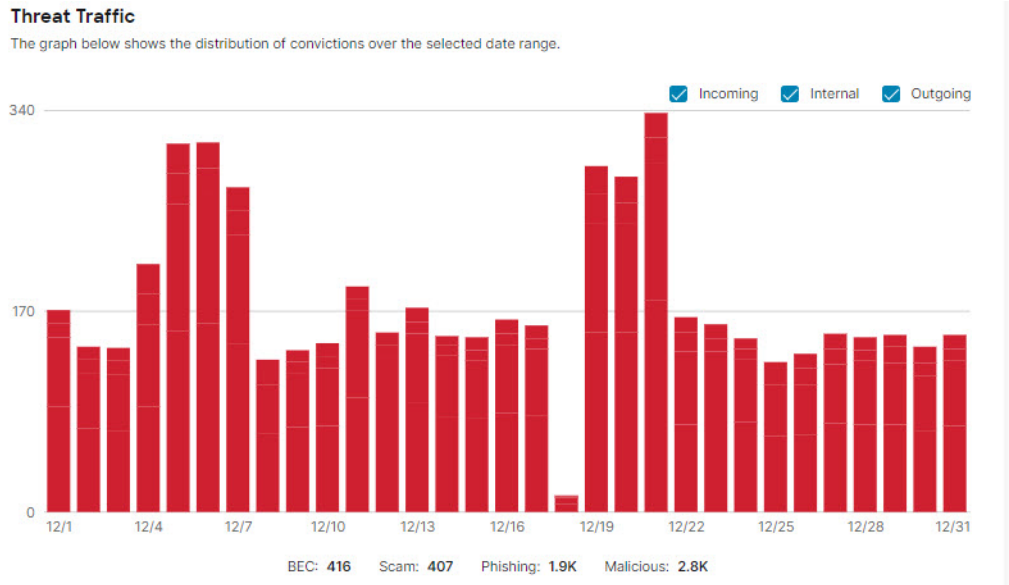
- 選択した30日間に Cisco Secure Email Threat Defense で検出された脅威メッセージおよび当該データの 1 年間の予測。1 年間の予測は、1 日の平均に 365 を掛けて計算されます。



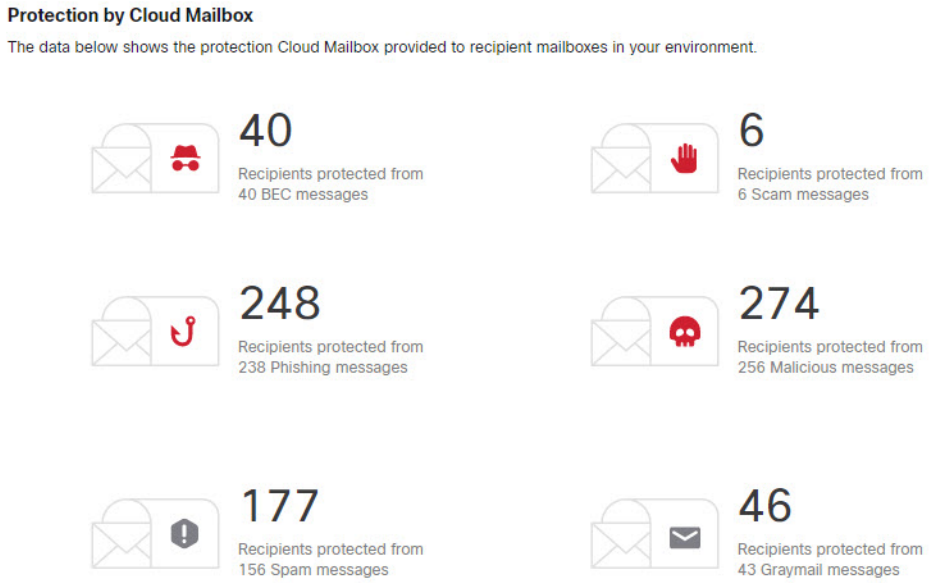
- [不要なメッセージ（Unwanted Messages）]。選択した30日間に検出されたスパムおよびグレイメールメッセージ、および当該データの 1 年間の予測。1 年間の予測は、1 日の平均に 365 を掛けて計算されます。



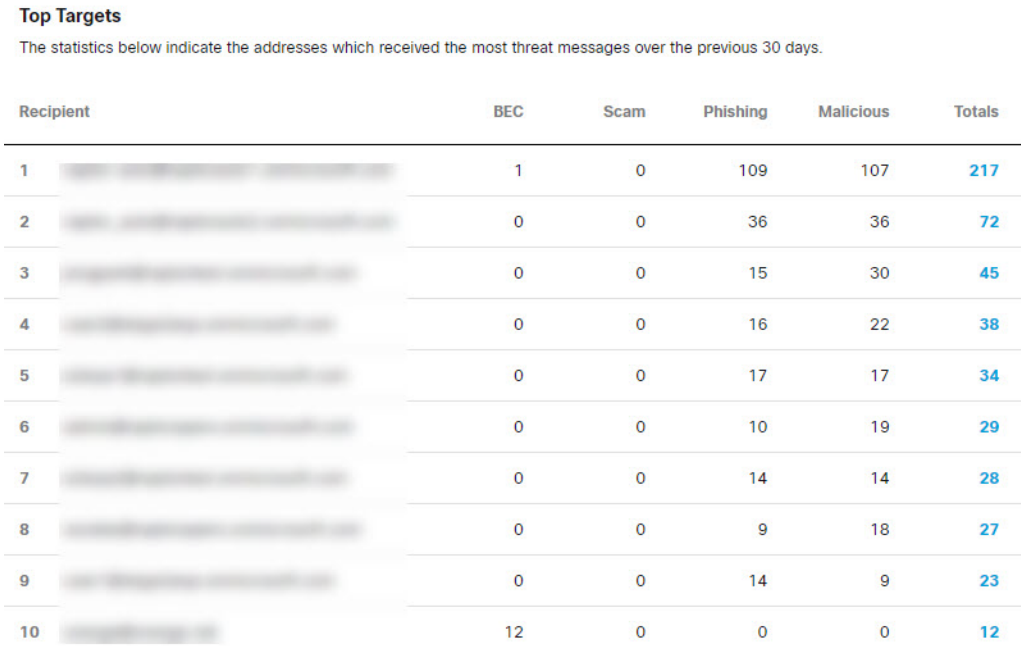
- [脅威トラフィック（Threat Traffic）]。このチャートには、選択した30日間の判定が表示されます。このチャートは宛先別にフィルタ処理できます。



- [Cisco Secure Email Threat Defenseによる保護(Protection by Secure Email Threat Defense)]。このチャートは、環境内の受信者のメールボックスに提供される保護 Cisco Secure Email Threat Defense を示しています。



- [上位ターゲット(Top Targets)]。このグラフには、選択した30日間における脅威メッセージの内部ターゲット上位 10 件が表示されます。



	Recipient	BEC	Scam	Phishing	Malicious	Totals
1	[redacted]	1	0	109	107	217
2	[redacted]	0	0	36	36	72
3	[redacted]	0	0	15	30	45
4	[redacted]	0	0	16	22	38
5	[redacted]	0	0	17	17	34
6	[redacted]	0	0	10	19	29
7	[redacted]	0	0	14	14	28
8	[redacted]	0	0	9	18	27
9	[redacted]	0	0	14	9	23
10	[redacted]	12	0	0	0	12

- 内部の脅威送信者。このチャートには、脅威メッセージの内部送信者上位 10 件が表示されます。

Internal Threat Senders

The internal addresses listed here were seen sending malicious or phishing messages from within the organization.

	Sender	Number of Messages Sent
1	[redacted]	54
2	[redacted]	50
3	[redacted]	16
4	[redacted]	2

影響力の高い人員リスト

経営幹部チームのメンバーなどの重要人物は、他のターゲットを侵害しようとして、なりすましを受ける危険にさらされています。影響力の高い人員リストは、Cisco Secure Email Threat Defense がなりすまし攻撃から組織を保護するのに役立ちます。

管理者は、最大 100 人のリストを作成して Cisco Talos に送信し、表示名と送信者の電子メールアドレスをさらに精査する必要があります。個人用に構成された情報からの逸脱は、有害と判定されたメッセージの [判定の詳細(Verdict Details)] パネルで [テクニック(Technique)] として識別されます。

影響力の高い人員リストにユーザーを追加する

次の手順を実行して、影響の高い人員リストにユーザーを追加します。

1. **[管理(Administration)]** > **[影響の高い人員(High Impact Personnel)]** を選択します。
2. [新しい人員を追加(Add New)] ボタンをクリックします。
3. ユーザー情報を入力します。名、姓、電子メールアドレスは必須です。
4. [送信(Submit)] をクリックして、リストへのユーザーの追加を完了します。

影響力の高い人員リストのユーザー情報を更新する

次の手順を実行して、影響の高い人員リストのユーザー情報を編集します。

1. **[管理(Administration)]** > **[影響の高い人員(High Impact Personnel)]** を選択します。
2. [アクション(Actions)] 列で、[編集(Edit)](鉛筆)ボタンをクリックします。
3. 必要に応じてユーザー情報をアップデートします。名、姓、電子メールアドレスは必須です。
4. [送信(Submit)] をクリックして、ユーザー情報の編集を終了します。

影響力の高い人員リストからユーザーを削除する

次の手順を実行して、影響の高い人員リストからユーザーを削除します。

1. **[管理(Administration)]** > **[影響の高い人員(High Impact Personnel)]** を選択します。
2. [アクション(Actions)] 列で、[削除(Delete)] ボタンをクリックします。
3. [削除の確認(Confirm Removal)] ダイアログで [削除(Delete)] をクリックし、アクションを完了します。

影響力の高い人員リストからユーザーを削除する

ユーザーの管理

[管理(Administration)] > **[ユーザー(Users)]** ページからユーザーアカウントを管理します。

Cisco Secure Email Threat Defense は、ユーザー認証管理に Cisco Security Cloud Sign On(旧 SecureX サインオン)を使用します。Security Cloud Sign On サインオンの詳細については、https://cisco.com/go/securesignon を参照してください。

注:既存の Cisco XDR、Cisco Secure Malware Analytics(旧 Threat Grid)、または Cisco Secure Endpoint(旧 AMP)のお客様は、必ず既存の Security Cloud Sign On ログイン情報でサインインしてください。既存のユーザーでない場合は、新しい Security Cloud Sign On アカウントを作成する必要があります

Security Cloud Sign On を使用すると、他のタイプのアカウントでサインオンできますが、シスコのセキュリティ製品アカウントの接続状態を維持するために、Security Cloud Sign On アカウントを使用することをお勧めします。

マルチアカウントアクセス

同じ Security Cloud Sign On アカウントを使用して、複数の Cisco Secure Email Threat Defense インスタンスにアクセスできます。これにより、一旦ログアウトしてから別の Security Cloud Sign On アカウントを使用して再度ログインすることなく、各インスタンスを簡単に追跡できます。

新規ユーザーの作成(50 ページ)の手順に従って、ユーザーを付加的な Cisco Secure Email Threat Defense インスタンスに追加します。同じ Security Cloud Sign On アカウントを使用しているアカウントは、[ユーザー(User)] メニューから利用できます。このアクセスは同じリージョン(北米、ヨーロッパ、オーストラリア、インド)の Cisco Secure Email Threat Defense インスタンスに限定されることに注意してください。

ユーザーロール

ロールベース アクセス コントロール(RBAC)により、アプリケーション内で異なるレベルの制御権またはアクセス権を持つユーザーを設定できます。Cisco Secure Email Threat Defense 次の表に示すロールに属するユーザーを作成できます。

表 1　　ユーザーの役割

ロール	説明
super-admin	これらのユーザーは、Cisco Secure Email Threat Defense のすべての機能にアクセスできます。設定やポリシーの変更、メッセージの再分類や修復、EML ファイルのダウンロード、電子メールメッセージのプレビュー表示が可能です。
admin	これらのユーザーは、スーパー管理者または管理者ユーザーを作成、編集、または削除できないことを除いて、スーパー管理者のすべての機能を備えています。
analyst	これらのユーザーは、検索およびインサイト機能を使用できます。メッセージの再分類と修復はできますが、ユーザーのメールボックスからメッセージを削除することはできません。アカウント設定やポリシーの変更、新規ユーザーの作成、編集、削除はできません。また、EML ファイルをダウンロードしたり、電子メールメッセージのプレビューを表示したりすることもできません。
read-only	これらのユーザーは、検索およびインサイト機能を使用できます。メッセージの再分類や修復、アカウント設定やポリシーの変更、新規ユーザーの作成はできません。また、EML ファイルをダウンロードしたり、電子メールメッセージのプレビューを表示したりすることもできません。

表 2　　役割別の機能へのアクセス

機能グループ	機能	役割
管理	ユーザーの追加/編集	■ super-admin ■ admin
	管理者の作成/編集/削除	■ super-admin
Business	Google アナリティクスの切り替え	■ super-admin ■ admin
	通知電子メールの表示	■ super-admin ■ admin
	レトロ通知電子メールの編集	■ super-admin ■ admin
	監査ログのダウンロード	■ super-admin ■ admin ■ analyst ■ read-only
	検疫フォルダの表示	■ super-admin ■ admin
	通知の表示	■ super-admin ■ admin ■ analyst ■ read-only
ポリシー	ポリシーの編集	■ super-admin ■ admin
	ドメインのインポート	■ super-admin ■ admin
	メッセージルールの変更	■ super-admin ■ admin ■ analyst
Search	ホームページから検索	■ super-admin ■ admin ■ analyst ■ read-only

表 2　　役割別の機能へのアクセス

機能グループ	機能	役割
メッセージ	展開の表示	■ super-admin ■ admin ■ analyst ■ read-only
	レポートの表示	■ super-admin ■ admin ■ analyst ■ read-only
	EML のダウンロード	■ super-admin ■ admin
	電子メールのプレビュー表示	■ super-admin ■ admin
再分類と修復	再分類	■ super-admin ■ admin ■ analyst
	メッセージの移動	■ super-admin ■ admin ■ analyst
	メッセージの隔離	■ super-admin ■ admin ■ analyst
	メッセージの削除	■ super-admin ■ admin
	修復エラーログの表示	■ super-admin ■ admin ■ analyst ■ read-only

表 2　　役割別の機能へのアクセス

機能グループ	機能	役割
Cisco XDR	ダッシュボードの承認	■ super-admin ■ admin
	リボンの承認	■ super-admin ■ admin ■ analyst ■ read-only
API	[アクセスAPI(Access API)] タブ	■ super-admin ■ admin
	アクセス API キー	■ super-admin ■ admin
	API ログイン情報の生成	■ super-admin ■ admin

新規ユーザーの作成

次の手順を実行して、新規ユーザーを作成します。

1. **[管理(Administration)]** > **[ユーザー(Users)]** の順に選択します。
2. [新規ユーザーを追加(Add New User)] をクリックします。
3. ユーザーのログイン情報を入力し、ロールを選択して、[作成(Create)] をクリックします。

   注: ユーザーの電子メールアドレスは、そのユーザーの Security Cloud Sign On アカウントの電子メールアドレスと*必ず*一致する必要があります。

ユーザーに「**Welcome toCisco Secure Email Threat Defense**」という件名の電子メールが配信されます。ユーザーは電子メールの指示に従って Security Cloud Sign On アカウントをセットアップし(まだアカウントを持っていない場合)、ログインする必要があります。

ユーザの編集

ユーザーのロールを更新できます。ユーザーの電子メールアドレスは編集できません。ユーザーが名前を変更した場合は、Security Cloud Sign On アカウントで名前を更新する必要があります。

ユーザーのロールを編集するには、次の手順を実行します。

1. **[管理(Administration)]** > **[ユーザー(Users)]** の順に選択します。
2. [アクション(Action)] 列の下にある鉛筆アイコンをクリックします。
3. [ユーザーの編集(Edit User)] ダイアログで、ユーザーの新しいロールを選択し、**[変更の保存(Save changes)]** をクリックします。

ユーザの削除

ユーザーを削除するには、次の手順を完了します。

1. **[管理（Administration）]** > **[ユーザー（Users）]** の順に選択します。
2. [アクション（Action）] 列の下にある X アイコンをクリックします。
3. [削除の確認（Confirm Deletion）] ダイアログで [削除（Delete）] をクリックし、アクションを完了します。

削除が完了したことを示すステータスメッセージが表示されます。これにより、Cisco Secure Email Threat Defense からユーザーのアカウントが削除されますが、Security Cloud Sign On アカウントは削除されません。複数の Cisco Secure Email Threat Defense インスタンスからユーザーを削除する場合は、インスタンスごとにこれらの手順を完了する必要があります。

ユーザの削除

ユーザー設定

個々のユーザープロファイルの設定には、[ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] からアクセスできます。

詳細

詳細セクションには、ユーザー名、役割、および組織が含まれています。

初期設定

[初期設定(Preferences)] セクションには、XDR リボンの承認とテーマの外観設定が含まれます。

XDR リボン

Secure Email Threat Defense は、Cisco XDR リボンと統合されています。リボンを使用すると、シスコのセキュリティ製品間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりできます。XDR リボンはユーザーごとに承認されます。詳細については、Cisco XDR(63 ページ)を参照してください。

テーマ

Secure Email Threat Defense の表示を明るい背景または暗い背景とするように選択できます。モードを切り替えるには、[ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] > [初期設定(Preferences)] > [テーマ(Theme)] に移動します。このガイドの画像は、通常、ライトテーマで表示されます。

初期設定

管理設定

このセクションで説明する管理設定には、**[管理(Administration)]** > **[ビジネス(Business)]** からアクセスできます。

アカウント

[アカウント(Account)] セクションには次の情報が表示されます。

- Microsoft 365 のテナント ID
- ジャーナルアドレス
- 会社 ID
- 検疫フォルダ ID
- サブスクリプション ID のサポート

ライセンス

[ライセンス(License)] セクションには次の情報が表示されます。

- ライセンスのタイプ
- シート数
- 開始日(スイートに含まれないスタンドアロンビジネスの場合)
- 終了日(スイートに含まれないスタンドアロンビジネスの場合)

初期設定

[初期設定(Preferences)] セクションには、通知電子メールアドレス、監査ログへのアクセス、Google アナリティクスの設定、およびビジネスレベルの Cisco XDR 統合承認が含まれます。

通知メール

通知メールアドレスは、Secure Email Threat Defense が電子メールを送信するアドレスです。たとえば、システムの更新、新機能、定期メンテナンスなどに関する通知を送信する場合があります。最初は初期ユーザーの電子メールに設定されます。

レトロスペクティブな判定の通知を通知電子メールアドレスに送信するかどうかを選択できます。レトロスペクティブな判定がメッセージに適用されると、電子メールが送信されます。

監査ログ

監査ログですべてのセキュリティイベントやセキュリティインシデントを継続的に追跡し、その影響を可視化します。過去3ヵ月間の監査ログを（月ごとに）CSV ファイル形式でエクスポートできます。監査ログをダウンロードするには、ドロップダウンから日付範囲を選択し、[CSVのダウンロード（Download CSV）] をクリックします。CSV には、イベントカテゴリ、日時、実行されたアクション、ユーザーの電子メールと IP、イベントステータスとメタデータに関する情報が記載されています。

Google アナリティクス

Google アナリティクスは、Secure Email Threat Defense を設定して利用規約に同意すると、最初に有効または無効になります。有効にすると、シスコは個人を特定できない使用状況データ（送信者、受信者、件名、URL など）が収集して、そのデータを Google アナリティクスと共有する場合があります。このデータにより、シスコは Secure Email Threat Defense がユーザーのニーズにどのように対応しているかをよりよく理解できるようになります。

Cisco XDR

Secure Email Threat Defense は Cisco XDR と統合されています。XDR を使用すると、その他のシスコのセキュリティ製品からのデータと一緒に Secure Email Threat Defense の情報を確認できます。この設定の詳細については、**Cisco XDR（63 ページ）**を参照してください。

メッセージルール

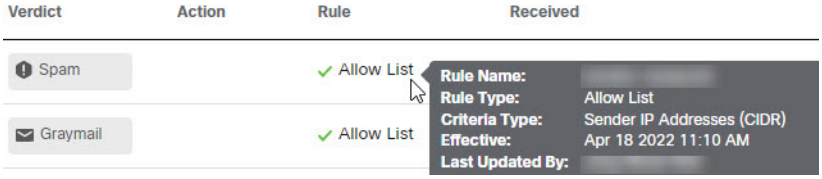
メッセージルールを使用すると、一部のタイプのメッセージを修復またはスキャンしないように指定できます。以下のものを作成できます。

- 許可リストルール
- 判定のオーバーライドルール
- バイパス分析ルール

注: [許可リスト（Allow List）] および [判定のオーバーライド（Verdict Override）] ルールは、認証なしモードのビジネスでは使用できません。

[管理（Administration）] > **[メッセージルール（Message Rules）]** ページから、メッセージルールを作成および管理します。

バイパス分析ルールは、許可リストルールと判定のオーバーライドルールよりも優先されます。メッセージがルールの影響を受ける場合は、[メッセージ（Messages）] ページの [メッセージルール（Message Rules）] 列に表示されます。[ルール（Rule）] 列の項目にカーソルを合わせると、適用されたルールが表示されます。



注: ルールはサブドメインに自動的に適用されません。ドメインは、ルールに示されているとおりに正確に一致します。

許可リストルール

許可リストルールを使用すると、特定の送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレスからの脅威、スパム、およびグレイメールメッセージの修復を防ぐことができます。メッセージは引き続き分析されますが、自動修復は適用されません。たとえば、Cisco Secure Email Threat Defense で特定の送信者からのアイテムがスパムであると判断されたものの、そのアイテムをユーザーの受信トレイに残しておきたい場合は、許可リストルールを作成して、該当するメッセージを修正するポリシーをオーバーライドできます。許可リストルールは、全体的なポリシー設定の例外として機能します。許可リストルールに一致するメッセージは、引き続き影響レポートに表示されます。

許可リストルール:

- 脅威、スパム、グレイメールに適用します。
- 許可された送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレス（IPv4 または CIDR ブロック）を指定します。
- ルールごとに最大 50 の基準を設定できます。つまり、50 個の電子メールアドレス、ドメイン、またはアドレスを設定できます。

アクティブなルールは 20 に制限されています。ルールは非アクティブ化または削除できます。

判定のオーバーライドルール

判定のオーバーライドルールを使用すると、ルールで指定された基準に一致する脅威、スパム、およびグレイメールの判定をオーバーライドできます。メッセージは「ニュートラル（Neutral）」判定とマークされ、修正されません。判定がオーバーライドされたメッセージは、影響レポートに表示されません。

判定のオーバーライドルール：

- 脅威、スパム、グレイメールに適用します。
- 許可された送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレス（IPv4 または CIDR ブロック）を指定します。
- ルールごとに最大 50 の基準を設定できます。つまり、50 個の電子メールアドレス、ドメイン、または IP アドレスを設定できます。

アクティブなルールは 20 に制限されています。ルールは非アクティブ化または削除できます。

バイパス分析ルール

バイパス分析ルールを使用すると、フィッシングテストまたは基準に一致するセキュリティ メールボックス メッセージの分析をバイパスできます。ルール基準を満たすメッセージによってすべてのエンジン分析がバイパスされるため、エンジンに干渉することなくセキュリティテストを処理できます。添付ファイルとリンクは、Cisco Secure Email Threat Defense によって開かれたりスキャンされたりしません。

注：テスト用にバイパス分析ルールを作成した場合は、脆弱性を防ぐために適切な期間が経過した後にルールを再検討する必要があります。

フィッシングテストルール：

- 指定した送信者の電子メールアドレス、送信者のドメイン、または IP アドレス（IPv4 または CIDR ブロック）から送信されたすべての受信メッセージに適用します。メッセージは分析されません。

  注：送信者 IP アドレス/CIDR 基準のみを使用して、特定の送信者インフラストラクチャをバイパスすることを推奨します。IP アドレスは、送信者の電子メールアドレスやドメインほど簡単にスプーフィングされることはありません。

- ルールごとに最大 50 の基準を設定できます。

セキュリティ メールボックス ルール：

- 指定した受信者の電子メールアドレスの受信メッセージに適用します。メッセージは分析されません。

  注：指定した受信者がメッセージの唯一の受信者である場合、セキュリティ メールボックス ルールが適用されます。他の受信者がコピーされているか、BCC（ブラインドカーボンコピー）として含まれている場合、メッセージは分析エンジンをバイパスしません。

- ルールごとに最大 50 の基準を設定できます。

アクティブなバイパス分析ルールは 20 に制限されています。ルールは非アクティブ化または削除できます。

バイパスルールの作成と使用に関するアドバイザリ

バイパスルールを作成および使用する場合は、次の重要な注意事項に留意してください。

- バイパスルールによって、ルール条件に一致するメッセージのスキャンと保護がすべてバイパスされます。顧客の従業員に対するセキュリティ認識トレーニング（フィッシングテスト）以外のユースケース、または組織のセキュリティ メールボックスに送信されるエンド メールボックス ユーザーからの報告には、バイパスルールを使用しないでください。これらは、バイパスルールでサポートされている唯一のシナリオです。他のすべてのシナリオでは、判定のオーバーライドルールまたは許可ルールのみがサポートされます。

- バイパスルールの基礎として、フィッシングテストベンダーが提供する専用の送信者 IP アドレス/CIDR ブロックのみを使用することを強く推奨します。
- フィッシングテストベンダーが専用の送信者 IP アドレス/CIDR ブロックを提供できない場合は、バイパスルールの送信者ドメインまたは電子メールアドレスを使用すると、スプーフィングされた可能性のあるメッセージをバイパスできます。
- 送信者の電子メール認証が、組織のアップストリームエッジ電子メール制御によって強力に適用されていること、および指定された送信者ドメインまたは送信者電子メールアドレスが、バイパスルールと一致させることを目的とするすべてのメッセージの最後の Return-Path ヘッダーと完全に一致していることを個別に検証した場合を除き、バイパスルールの送信者ドメインまたは電子メールアドレスは使用しないでください。

メッセージルールの追加

メッセージルールを追加する手順は、ルールのカテゴリによって若干異なります。

新しい許可リストまたは判定のオーバーライドルールの追加

新しいルールを作成するには、次の手順を実行します。

1. **[管理(Administration)]** > **[メッセージルール(Message Rules)]** の順に選択します。
2. 作成するルールのカテゴリを、[許可リスト(Allow List)] または [判定オーバーライド(Verdict Override)] のいずれかから選択します。
3. [新規ルールの追加(Add New Rule)] ボタンをクリックします。
4. ルール名を作成します。各ルールには固有の名前が必要です。
5. 基準のタイプを選択します。送信者の電子メール、送信者のドメイン、送信者の IP アドレス(IPv4)、または送信者の IP アドレス(CIDR)を選択できます。
6. 許可またはオーバーライドする項目をカンマで区切って入力します。
7. 許可する判定に応じて、スパム、グレイメール、脅威を選択します。
8. [送信(Submit)] をクリックして、ルールの作成を終了します。

ルールがリストに追加されます。変更が適用されるまでに最大で 20 分かかる場合があります。

新しいバイパス分析ルールの追加

新しいルールを作成するには、次の手順を実行します。

1. **[管理(Administration)]** > **[メッセージルール(Message Rules)]** の順に選択します。
2. [バイパス分析(Bypass Analysis)] を選択します。
3. [新規ルールの追加(Add New Rule)] ボタンをクリックします。
4. ルール名を作成します。各ルールには固有の名前が必要です。
5. 作成するルールタイプを、[フィッシングテスト(Phish Test)] または [セキュリティメールボックス(Security Mailbox)] のいずれかから選択します。

6. [フィッシングテスト(Phish Test)] ルールの場合は、基準タイプを [送信者の電子メールアドレス(Sender Email Addresses)] または [送信者のドメイン(Sender Domains)]、[送信者のIPアドレス(IPv4)(Sender IP Addresses (IPv4))]、[送信者のIPアドレス(CIDR)(Sender IP Addresses (CIDR))] のいずれかから選択します。次に、コンマで区切って項目を入力します。

   [セキュリティメールボックス(Security Mailbox)] ルールの場合は、受信者の電子メールアドレスをコンマで区切って入力します。

7. [送信(Submit)] をクリックして、ルールの作成を終了します。

ルールがリストに追加されます。変更が適用されるまでに最大で 20 分かかる場合があります。

注: テスト用にバイパス分析ルールを作成した場合は、脆弱性を防ぐために適切な期間が経過した後にルールを再検討する必要があります。バイパスルールを作成および使用する際に留意すべき、重要な注意事項を参照してください。

ルールの編集

編集できるのは有効なルールのみです。規則を編集するには、次の手順を実行します。

1. **[管理(Administration)]** > **[メッセージルール(Message Rules)]** の順に選択します。
2. 編集するルールのタイプを選択します。
3. [アクション(Action)] 列で、編集するルールの横にある鉛筆アイコンをクリックします。
4. 必要な変更を行ったら、[変更の保存(Save Changes)] をクリックします。

ルールが更新されます。変更が適用されるまでに最大で 20 分かかる場合があります。

ルールの有効化または無効化

既存のルールを有効または無効にするには、次の手順を実行します。

1. **[管理(Administration)]** > **[メッセージルール(Message Rules)]** の順に選択します。
2. 有効または無効にするルールのタイプを選択します。
3. [アクション(Action)] 列で、ステータスを変更するルールの横にある有効または無効アイコンをクリックします。

ルールのステータスが更新されます。変更が適用されるまでに最大で 20 分かかる場合があります。

ルールの削除

ルールを削除するには、次の手順に従います。

1. **[管理(Administration)]** > **[メッセージルール(Message Rules)]** の順に選択します。
2. 削除するルールのタイプを選択します。
3. [アクション(Actions)] 列で、削除するルールの横にある削除アイコンをクリックします。

ルールが削除されます。

Microsoft 許可リストと安全な送信者

Cisco Secure Email Threat Defense は、スパムおよびグレイメールメッセージに関して、Microsoft 365 のスパムフィルタ許可リストに追加された送信者とドメインを受け入れます。MS 許可リストは、脅威の判定（BEC、詐欺、悪意がある、フィッシング）では使用されません。これらの項目は、ポリシー設定に従って修復されます。詳細については、『Cisco Secure Email Threat Defense FAQ: Secure Email Threat Defense and Microsoft 365』を参照してください。

個々のユーザーがメールボックス内の許可リストを設定することを組織が許可している状況で、特定のメッセージがユーザーの許可リストに含まれる場合、Microsoft 許可リストが Cisco Secure Email Threat Defense で常に適用されることはありません。Cisco Secure Email Threat Defense でこれらの設定を適用する場合は、[ポリシー（Policy）] ページの [スパムまたはグレイメールと判定されたMicrosoft Safe Senderメッセージを修復しない（Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts）] チェックボックスをオンにします。Safe Sender フラグは、スパムとグレイメールの判定では適用されますが、悪意とフィッシングの判定では適用されません。つまり、スパムまたはグレイメールと判定された Safe Sender メッセージは修正されません。

Microsoft 許可リストと安全な送信者

Cisco XDR

Cisco XDR は、シスコのセキュリティ製品を統合プラットフォームに接続します。Secure Email Threat Defense は、Cisco XDR および Cisco XDR リボンと統合されています。

- XDR を使用すると、その他のシスコのセキュリティ製品からのデータと一緒に Secure Email Threat Defense の情報を確認し、アクションを実行できます。
- XDR リボンを使用すると、シスコのセキュリティ製品間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりできます。

このドキュメントに記載されていない XDR の詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/）を参照してください。

XDR

Secure Email Threat Defense には、Cisco XDR ダッシュボードで表示できる次のタイルがあります。

- [宛先別メッセージ（Messages by direction）]：電子メールトラフィックの合計が宛先別に表示されます。電子メールは、[送信（Outgoing）]、[内部（Internal）]、および [受信（Incoming）] に分けられます。
- [脅威（Threats）]：BEC、詐欺、フィッシング、または悪意のあると判定されたメッセージのスナップショットが表示されます。
- [スパム（Spam）]：スパムと判定されたメッセージのスナップショットが表示されます。
- [グレイメール（Graymail）]：グレイメールと判定されたメッセージのスナップショットが表示されます。

XDR ダッシュボードの詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/）を参照してください。

Secure Email Threat Defenseの Cisco XDR の承認

Secure Email Threat Defense の Cisco XDR を承認するには、Cisco XDR のアカウントを持ち、Cisco XDR 組織の一員となる必要があります。詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/）を参照してください。

注：Secure Email Threat Defense アカウントは、一度に 1 つの Cisco XDR 組織とのみ統合できます。

Secure Email Threat Defense のネットワーク管理者および管理者ユーザーは、Secure Email Threat Defense インスタンス向けに Cisco XDR モジュールを承認できます。

1. **[管理（Administration）]** > **[ビジネス（Business）]** の順に選択します。
2. **[初期設定（Preferences）]** > **[Extended Detection and Response]** で、**[XDR統合の承認（Authorize XDR Integration）]** をクリックします。
3. 承認フローを完了します。

XDR 設定が成功したことを示すバナーが表示されます。

XDR ダッシュボードに Secure Email Threat Defense のタイルを追加できるようになりました。その実行方法については、Cisco XDR のマニュアル（ https://docs.xdr.security.cisco.com/Content/Control-Center/configure-dashboards.htm）を参照してください。

Secure Email Threat Defenseの XDR 承認の取り消し

注: スーパー管理者または管理者ユーザーがこのタスクを実行できます。Secure Email Threat Defense インスタンス向けに XDR を承認したユーザーでなくてもこのタスクを実行できます。

XDR の承認を取り消すには、次の手順に従います。

1. **[管理(Administration)]** > **[ビジネス(Business)]** の順に選択します。
2. **[初期設定(Preferences)]** > **[Extended Detection and Response]** で、**[承認を取り消す(Revoke Authorization)]** をクリックします。

XDR 設定が正常に更新されたことを示すバナーが表示されます。

XDR リボン

XDR リボンはページの下部に配置されており、ご使用環境内で Secure Email Threat Defense とその他のシスコのセキュリティ製品間を移動しても保持されます。すべての Secure Email Threat Defense ユーザーは、XDR リボンの使用を承認できます。リボンを使用して、シスコのセキュリティ アプリケーション間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりします。

XDR リボンの詳細については、Cisco XDR のマニュアル(https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm)を参照してください。

ピボットメニュー

リボンを承認すると、Secure Email Threat Defense のメッセージレポート内に XDR ピボットメニューが追加されます。これらのメニューは、購入したシスコのセキュリティ製品に応じて、各オブザーバブルに関する追加情報にアクセスするための中心地点となります。

同様に、Cisco Secure Email Threat Defense と XDR の統合により、ピボットメニューを使用して XDR から Cisco Secure Email Threat Defense にアクセスできます。ピボットできる観測対象は次のとおりです。

- [電子メールアドレス(Email Address)]
- [電子メールメッセージID(Email Message ID)]
- [電子メールの件名(Email Subject)]
- [ファイル名(File Name)]
- [送信者IP(Sender IP)]
- [SHA 256(SHA 256)]
- [URL(URL)]

ピボットメニューを使用して、次の操作を実行します:

- 特定の監視可能なメッセージをピボットメニューから直接隔離します。Cisco Secure Email Threat Defense は、これらのメッセージが XDR ユーザーによって手動で修復されたことを示します。
  - **注:** ピボットメニューからの隔離は 100 メッセージまでに制限されています。
- 隔離したメッセージを受信トレイに戻します。Cisco Secure Email Threat Defense は、これらのメッセージが XDR ユーザーによって手動で修復されたことを示します。
  - **注:** 隔離から受信トレイへの移動は 100 メッセージまでに制限されています。

XDR のピボットメニューの詳細については、XDR のマニュアル(https://docs.securex.security.cisco.com/SecureX-Help/Content/pivot-menus.html)を参照してください

XDR リボンの承認

XDR リボンはユーザーレベルで承認されます。リボン内または [ユーザー設定(User Preferences)] メニューからリボンを承認できます。

注: リボンを承認する前に、XDR アカウントをアクティブ化する必要があります。これを行うには、Secure Email Threat Defenseの Cisco XDR の承認(63 ページ) の指示に従うか、他のモジュールを XDR に統合します。

XDR リボン内からの承認

リボン内から XDR リボンを承認するには、次の手順を実行します。

1. XDR リボンで **[XDRの取得(Get XDR)]** をクリックします。
2. [アプリケーションアクセスの許可(Grant Application Access)] ダイアログで、[Secure Email Threat Defenseリボンを承認(Authorize Secure Email Threat Defense Ribbon)] をクリックします。

XDR リボンが承認されました。XDR 設定が正常に更新されたことを示すバナーが表示されます。

Secure Email Threat Defense のユーザー設定からの承認

[ユーザー設定(User Settings)] メニューから XDR リボンを承認するには、次の手順を実行します。

1. [ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] を選択します。
2. **[初期設定(Preferences)]** > **[XDRリボン(XDR Ribbon)]** で、**[XDRリボンの承認(Authorize XDR Ribbon)]** をクリックします。
3. [アプリケーションアクセスの許可(Grant Application Access)] ダイアログで、[Cisco Secure Email Threat Defenseリボンを承認(Authorize Cisco Secure Email Threat Defense)] をクリックします。

XDR リボンが承認されました。XDR 設定が正常に更新されたことを示すバナーが表示されます。

XDR リボンの承認の取り消し

XDR リボンはユーザーレベルで承認されます。リボン内または [ユーザー設定(User Preferences)] メニューから承認を取り消すことができます。

XDR リボン内からの承認の取り消し

リボン内から XDR リボンの承認を取り消すには、次の手順を実行します。

1. XDR リボンで **[設定(Settings)]** > **[承認(Authorization)]** > **[取り消し(Revoke)]** を選択します。
2. [取り消し(Revoke)] ダイアログで、[確認(Confirm)] をクリックします。

XDR リボンが Secure Email Threat Defense ユーザーアカウントに対して承認されなくなりました。

Secure Email Threat Defense のユーザー設定からの承認の取り消し

[ユーザー設定(User Settings)] メニューから XDR リボンの承認を取り消すには、次の手順を実行します。

1. [ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] を選択します。
2. **[初期設定(Preferences)]** > **[XDRリボン(XDR Ribbon)]** で、**[承認を取り消す(Revoke Authorization)]** をクリックします。

XDR リボンが Secure Email Threat Defense ユーザーアカウントに対して承認されなくなりました。XDR 設定が正常に更新されたことを示すバナーが表示されます。

API

Cisco Secure Email Threat Defense API を使用すると、安全でスケーラブルな方法でプログラムからデータにアクセスして使用することができます。詳細については、API ドキュメント https://developer.cisco.com/docs/message-search-api/ を参照してください。

Secure Email Threat Defense の無効化

メッセージの送信元：Microsoft 365

メッセージの送信元が Microsoft の場合に Cisco Secure Email Threat Defense を非アクティブ化するには、主に次の 2 つのタスクがあります。

- Microsoft 365 管理センターから Cisco Secure Email Threat Defense ジャーナルエントリを削除する
- Microsoft Azure テナントから Cisco Secure Email Threat Defense アプリケーションを削除する

Cisco Secure Email Threat Defense ジャーナルルールの削除

Cisco Secure Email Threat Defense ジャーナルルールの削除方法：

1. Microsoft 365 管理センター（https://admin.microsoft.com/AdminPortal/Home#/homepage）に移動します。
2. [管理センター（Admin centers）] > [コンプライアンス（Compliance）] > [データライフサイクル管理（Data lifecycle management）] > [Exchange（レガシー）（Exchange (legacy)）] > [ジャーナルルール（Journal rules）] の順に移動します。
3. Cisco Secure Email Threat Defense ジャーナルルールを選択して、[削除（Delete）] をクリックします。[はい（Yes）] を選択して、ジャーナルルールを削除することを確認します。

Azure からの Cisco Secure Email Threat Defense アプリケーションの削除

Azure から Cisco Secure Email Threat Defense アプリケーションを削除する方法：

1. portal.azure.com に移動します。
2. [エンタープライズアプリケーション（Enterprise applications）] を見つけて選択します。

   注：Azure で古いビューを使用している場合、これは**アプリの登録**と呼ばれることがあります。
3. **Cisco Secure Email Threat Defense** または **Cisco Secure Email Threat Defense（読み取り専用）**アプリケーションを見つけて選択します。
4. 左側のペインで、[プロパティ（Properties）]を選択します。
5. [削除（Delete）] ボタンをクリックしてから [はい（Yes）] を選択し、Secure Email Threat Defense アプリを削除することを確認します。

メッセージの送信元：ゲートウェイ

メッセージの送信元にゲートウェイを使用しているときに Cisco Secure Email Threat Defense を非アクティブ化するには、主に次の 2 つのタスクがあります。

- Cisco Secure Email Threat Defense へのメッセージの送信を停止するようにゲートウェイを設定する

- Microsoft Azure テナントから Cisco Secure Email Threat Defense アプリケーションを削除する（認証なしモードの場合は不要）

メッセージの送信を停止するようにゲートウェイを構成する

Cisco Secure Email Threat Defense へのメッセージの送信を停止するようにゲートウェイを設定する方法：

1. Cisco Secure Email Cloud Gateway コンソールで、[セキュリティサービス（Security Services）] > [Threat Defense Connector] に移動します。
2. [Threat Defense Connector] を [無効（Disabled）] に設定します。

Azure からの Cisco Secure Email Threat Defense アプリケーションの削除

Azure から Cisco Secure Email Threat Defense アプリケーションを削除する方法：

1. portal.azure.com に移動します。
2. [エンタープライズアプリケーション（Enterprise applications）] を見つけて選択します。

   注：Azure で古いビューを使用している場合、これは**アプリの登録**と呼ばれることがあります。
3. **Cisco Secure Email Threat Defense** または **Cisco Secure Email Threat Defense（読み取り専用）**アプリケーションを見つけて選択します。
4. 左側のペインで、[プロパティ（Properties）]を選択します。
5. [削除（Delete）] ボタンをクリックしてから [はい（Yes）] を選択し、Secure Email Threat Defense アプリを削除することを確認します。

よく寄せられる質問(FAQ)

よく寄せられる質問は Cisco Secure Email Threat DefenseFAQ で参照できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。